Diseminación Segura de Datos en Redes Inalámbricas de Sensores

Luis Enrique Palafox Maestre/José Antonio García Macias
Depto. de Ciencias de la Computación
CICESE Ensenada, B.C., Mexico
{palafox,jagm}@cicese.mx

1 Motivación

Actualmente, la mayoría de los esfuerzos en la investigación sobre WSNs son canalizados al diseño de protocolos eficientes en el uso de los recursos disponibles [1].

En general, la mayoría de los trabajos de investigación hasta la fecha se han realizado con la finalidad de poder contar con redes de sensores que sean funcionales en la práctica.

Sin embargo, más allá de la funcionalidad, un aspecto que no ha recibido la suficiente atención, es el aspecto de la seguridad de la información en las WSNs. Este aspecto introduce una serie de problemas que es necesario resolver para poder contar con redes de sensores adecuadas para diversos tipos de aplicaciones en los que se requiera proveer de servicios de confidencialidad y de autentificación con el fin de protegerse de posibles ataques de usuarios maliciosos.

2 Trabajo relacionado

A pesar de que existen varios problemas abiertos en la seguridad de redes inalámbricas de sensores, ya hay una cantidad significativa de trabajo relacionado, por cuestiones de espacio, únicamente se incluirá el que se considera más relevante para el tema de interés.

Przydatek et al. describen una técnica de agregación segura de datos a la que llamaron SIA [5]. En SIA se introduce una técnica basada en tres fases: agregar-asegurar-comprobar.

Hu y Evans proponen una técnica de agregación segura de datos que utiliza el protocolo μTESLA para ofrecer seguridad [2]. Sin embargo, esta técnica, no garantiza que los nodos y los agregadores se encuentren reportando datos correctos. Para atacar este problema, la estación base se responsabiliza de distribuir llaves temporales hacia la red asi como la llave utilizada por μTESLA. Al utilizar esta llave, los nodos pueden verificar los códigos MAC[1] de sus hijos.

[1] MAC = *Message Authentication Code*

71%	Transmisión de datos
20%	Transmisión de MAC
7%	Transmisión de enunciados (para ofrecer actualidad de datos)
2%	Cálculo de MAC y encriptación

Tabla 1. Costos de energía para agregar seguridad a una red de sensores [4]

Perrig y Tygar [2003] muestran que la introducción del MAC a la comunicación de datos no representa un costo excesivo. En la Tabla 1 se muestran los costos de agregar protocolos de seguridad a una red de sensores. La mayoría del incremento de energía es debido a la trasmisión de datos adicionales y no debido al costo computacional introducido por los algoritmos.

3 Objetivos

Se ha propuesto un objetivo general del cual se desprenden varios objetivos particulares. Se enlistarán ambos a continuación.

Objetivo general:

Proponer nuevos esquemas de diseminación de datos orientados a redes inalámbricas de sensores que ofrezcan los servicios de seguridad requeridos por las aplicaciones para prevenir, protegerse y recuperarse de posibles ataques que el medio y agentes externos pueden introducir a ella.

Objetivos particulares:

- Analizar el trabajo previo realizado sobre diseminación de datos y seguridad en redes inalámbricas de sensores.
- Explorar técnicas no convencionales para el diseño de técnicas de diseminación segura de datos en redes de sensores inalámbricas.

- Definir un esquema de pruebas de seguridad que puedan ser utilizadas como un patrón de medición de la eficiencia en el desempeño de los esquemas de diseminación propuestos.

- Realizar experimentos con los esquemas de diseminación propuestos obteniendo resultados satisfactorios en relación a otros trabajos previos realizados sobre diseminación de datos.

4 Metodología

En base a lo mostrado en la Tabla 1, se introduce la idea de que el transmitir únicamente el MAC desde los nodos de sensado hacia los agregadores se puede disminuir considerablemente el consumo de energía y a la vez mejorar el nivel de seguridad de la agregación de datos debido a que una vez recibido el código MAC por el agregador, se establece un compromiso entre este y los nodos imposibilitando así que las lecturas sean modificadas por algún posible ataque.

Con esta idea, la arquitectura presentada en este trabajo propone un nuevo esquema en el cual las lecturas tomadas por los sensores se clasificarán dentro de un intervalo cuyo tamaño es configurable a la precisión requerida por la aplicación especifica, es decir, en cuanto mayor precisión se requiera menor será el rango comprendido por los intervalos, una vez clasificadas las lecturas de los nodos en los intervalos previamente definidos, se enviaría únicamente el MAC perteneciente a cada intervalo hacia los agregadores.

Como ya se mencionó anteriormente, la naturaleza de las redes de sensores densamente pobladas comprende grandes cantidades de información redundantes, de tal manera, que se anticipa que un gran número de nodos pertenecientes a un mismo agregador presentan lecturas muy similares, por tal motivo, se prevé que el enviar el MAC únicamente en lugar de toda la información pueda traer un ahorro considerable en el costo de comunicación y por ende en el consumo de energía. Posteriormente, si existe un interés adicional por parte del agregador se pueden hacer peticiones específicas a los nodos de interés. Y una vez que el agregador reciba las lecturas de interés las puede autentificar ya que este tendría los MACs correspondientes almacenados en un buffer de memoria.

Los valores correspondientes a las lecturas que no fueron solicitadas pueden ser inferidos trivialmente por los agregadores ya que estos generaron códigos MAC redundantes.

Por otra parte, si se detecta violación en la seguridad, no se interrumpe el servicio como en el caso de otras propuestas presentadas sino que se pasa a modo de estimación. En este caso se utilizará una variante de un algoritmo de estimación ya propuesto [3]. Otra alternativa de respuesta a este tipo de ataque es que posteriormente se descarten todos los paquetes enviados por el nodo comprometido.

Los criterios para detectar violación en la seguridad es:

- Lecturas fuera de un rango determinado.

- Violación del esquema de autentificación.

5 Estado de la investigación

Debido a las limitantes de memoria se eligió el algoritmo CBC-MAC para obtener la huella del paquete de datos. Este algoritmo permite la reutilización de código para ofrecer servicios adicionales de seguridad tal como confidencialidad de los datos a ser transmitidos por los nodos hijos.

Dicho algoritmo está siendo implementado en una plataforma de redes de sensores basado en los motes de *Berkeley* tipo TMote Sky. Una vez implementado el protocolo de seguridad propuesto se evaluará utilizando el mátodo presentado en [6].

Parte del desempeño de la técnica propuesta depende del minimizar el número de colisiones generadas por la función MAC, ya que el hecho de que se presente una colisión se traduce en una falsa detección de datos redundantes en la red de sensores. Por esta razón, se han realizado simulaciones en Matlab del algoritmo mencionado para detectar posibles colisiones con la función MAC que pudieran afectar el desempeño de la técnica de diseminación de datos propuesta.

6 Resultados preliminares

Se capturaron datos reales durante dos horas utilizando una red de sensores formada por 10 motes TMote Sky, posteriormente fuera de línea se calculó el MAC mediante el algoritmo CBC-MAC con la idea de detectar colisiones en lecturas generadas de un ambiente real.

Después de realizar el cálculo del total de las muestras capturadas no se detectó colisión alguna, es decir, no se encontró ningún valor igual del MAC para lecturas diferentes.

Referencias

[1] D. E. Culler and W. Hong. Wireless sensor networks - introduction. *Commun. ACM*, 47(6):30–33, 2004.

[2] L. Hu and D. Evans. Secure aggregation for wireless network. In *SAINT Workshops*, pages 384–394. IEEE Computer Society, 2003.

[3] L. E. Palafox-Maestre and J. A. Garcia-Macias. A bio-inspired approach for data dissemination in wireless sensor networks. *INFOCOMP Journal of Computer Science (Accepted for publication)*, 2006.

[4] A. Perrig and J. Tygar. *Secure Broadcast Communication in Wired and Wireless Networks*. Kluwer Academic Publishers, 2003.

[5] B. Przydatek, D. X. Song, and A. Perrig. Sia: secure information aggregation in sensor networks. In I. F. Akyildiz, D. Estrin, D. E. Culler, and M. B. Srivastava, editors, *SenSys*, pages 255–265. ACM, 2003.

[6] D. Wagner. Resilient aggregation in sensor networks. In *SASN '04: Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor networks*, pages 78–87, New York, NY, USA, 2004. ACM Press.