C. Alcaraz, R. Roman, and J. Lopez, "Análisis de la Aplicabilidad de las Redes de Sensores para la Protección de Infraestructuras de Información Críticas", *VI Jornadas de Ingeniería Telemática (JITEL08)*, pp. 437, 2008.
NICS Lab. Publications: https://www.nics.uma.es/publications

Análisis de la Aplicabilidad de las Redes de Sensores para la Protección de Infraestructuras de Información Críticas

Cristina Alcaraz, Rodrigo Román, Javier López
Departamento de Lenguajes y Ciencias de la Computación
Universidad de Málaga
29071, Malaga, España
{alcaraz,roman,jlm}@lcc.uma.es

***Abstract*—Las infraestructuras críticas, como el sector energético, la banca, el transporte, y muchas otras, son un pilar esencial para en bienestar de la sociedad y la economía de un país. Estas infraestructuras dependen a su vez de ciertas infraestructuras de información, las cuales permiten su correcto funcionamiento. La tarea de proteger esas infraestructuras (de información) críticas es compleja y multidimensional, con una gran cantidad de desafíos por resolver. Precisamente, las redes de sensores pueden ser de gran ayuda para esta tarea, debido a sus capacidades de control distribuidas y a su habilidad de funcionar en situaciones extremas. Este artículo analiza la utilidad de las redes de sensores en este contexto, describiendo tanto sus capacidades como sus posibles roles y mecanismos de integración para la protección de infraestructuras (de información) críticas.**

I. Introducción

Dentro del marco de la Unión Europea, una infraestructura se considera como "una estructura de redes y sistemas interrelacionados entre sí, compuestas por industrias, instituciones (incluyendo personal y procedimientos), y medios de distribución que proporciona un flujo fiable de productos, mercancías y servicios que permiten el funcionamiento adecuado de los gobiernos, la economía, la sociedad, y otras infraestructuras" [1]. Habría también que considerar todos aquellos procedimientos de operación, prácticas de gestión, y políticas de desarrollo [2]. Ahora bien, cuando dicha infraestructura tiene una gran influencia sobre su entorno, tan fuerte que si no está disponible por un periodo de tiempo no trivial los posibles efectos de su malfuncionamiento serán importantes, se considera crítica. Aunque actualmente no existe una única definición del concepto de Infraestructuras Críticas (CI), la mayoría de las CI comparten cuatro propiedades: interdependencias, capital privado (la mayoría de las CI están en manos del sector privado), globalización, y dependencia de las tecnologías de la información (ICT).

Las ICT son también consideradas críticas, puesto que en la mayoría de los casos son indispensables para que las CI puedan funcionar, realizando operaciones de manejo, control, y supervisión [3]. De esta forma, surge el concepto de Infraestructura de Información Crítica (CII), y al igual que con las CI, no existe una definición exacta del término CII, probablemente porque las tecnologías de la información son consideradas simplemente una parte esencial de las CI. Esto se corresponde con la definición dada por el proyecto Europeo FP6 CI2RCO, donde las CII son "procesos de información respaldados por tecnologías de la información los cuales forman CI por sí mismos o que son críticos para el funcionamiento de otras CI" [1]. De todas formas, es necesario puntualizar la separación entre ambas debido a la naturaleza inmaterial de las amenazas específicas que pueden afectar a una CII y a los elementos afectados por esas amenazas: el flujo de información de la infraestructura, el conocimiento derivado de ese flujo de información, y los servicios proporcionados a causa de dicho conocimiento [4]. Realizando esta separación conceptual, es posible tener una idea más clara de qué retos deben superarse para proteger estas CII.

Por otro lado, la Protección de Infraestructuras de Información Críticas (CIIP) puede ser definida de la forma siguiente: "Los programas y actividades realizados por los dueños de las infraestructuras, usuarios, operadores, instituciones de investigación, gobiernos, y autoridades regulatorias que persiguen el mantenimiento de la funcionalidad de las infraestructuras (de información) críticas en caso de fallos, ataques o accidentes encima de un nivel mínimo de servicio y procurando minimizar tanto el tiempo de recuperación como el daño sufrido" [1]. Por consiguiente, la protección de una CII es esencial para proteger una CI debido a la dependencia con las ICT.

Una de las tecnologías que pueden ser aplicadas para proteger esas CI son las redes de sensores [5], las cuales pueden abstraerse como la "piel" de un sistema informático, sintiendo información de su entorno (temperatura, humedad, luz o radiación). Una red de sensores puede funcionar como un sistema redundante y fiable, que proporciona un diagnóstico de un entorno determinado. Además, también puede sentar las bases de un sistema distribuido de control inteligente, capaz de generar avisos para prevenir situaciones extremas, localizar el problema, y ser capaz de autoconfigurarse.

Aunque sus dispositivos presentan restricciones importantes relacionados con el microprocesador, memoria, transceptor y batería, éstos son apropiados para ser aplicados en cualquier

tipo de aplicación, desde sistemas simples (p. ej. monitorización del medio) hasta sistemas complejos o críticos (p. ej. monitorización de puentes o minas de carbón). De hecho, el objetivo de este artículo será analizar la utilidad de ésta tecnología como un sistema de apoyo que pueda ayudar a la CIIP. De hecho, en la sección 2 se analizará la aplicabilidad de estas redes a la CIIP junto a iniciativas relacionadas con este campo. La sección 3 muestra las líneas de investigación actuales en la seguridad de las redes de sensores y las líneas a seguir para su integración en las CI, y en la sección 4 concluye el artículo.

II. Redes de Sensores en CIIP

Como ya se ha mencionado anteriormente, una de las tecnologías más apropiadas para la CIIP, hoy en día, son las redes de sensores, debido a sus características inherentes, como la monitorización continuada del medio y por sus capacidades para funcionar bajo condiciones adversas. También, son capaces de generar alarmas en situaciones críticas, y pueden proveer las localizaciones exactas del problema para ayudar en los procesos de mantenimiento, o quizás de reparación lo antes posible.

Estas particularidades no sólo son atractivas para la comunidad científica sino para la propia industria y los gobiernos. Por ejemplo, en el año 2004, el departamento de seguridad nacional (Homeland Security) de los Estados Unidos declaró un plan Nacional para la Investigación y Desarrollo (I+D) para la protección de las CI mediante puntos estratégicos registrados en *Common Operating Picture* (COP). También, el gobierno Australiano estableció un plan de I+D, a través de la red de investigación para una Australia segura (*Research Network for a Secure Australia*, RNSA), conocido como Centro de Investigación Cooperativa para la Seguridad (*Cooperative Research Center for Security* (CRC-SAFE)). Dentro de su programa, una de las iniciativas es aplicar sistemas electrónicos (como las redes de sensores) [6] seguros para la protección de las CI.

No obstante, las redes de sensores necesitan de sistemas adicionales que prevean situaciones anómalas y permitan la reconfiguración de los diferentes componentes afectados de la infraestructura. Estos sistemas necesitan de los datos percibidos de la red distribuida, con el objeto de ayudar en los procesos de reactivación de las zonas o componentes afectados (quizás por congestión o fallo), permitiendo un control exhaustivo del sistema cuando se presenten situaciones donde no esté disponible un sistema central especializado en la gestión de datos. Concretamente, estos sistemas adicionales son, por un lado, los sistemas de aviso temprano (*Early Warning System* (EWS)), los cuales analizan los datos percibidos del medio, y detectan situaciones anómalas y posiblemente cercanas. Un ejemplo de su uso sería detectar inundaciones en comunidades con pobres infraestructuras, trabajo realizado por un grupo de investigadores del Instituto Tecnológico de Massachusetts [7]. Por otro lado, están los sistemas de reconfiguración dinámica (*Dynamic Reconfiguration System* (DRS)), los cuales reconfiguran las partes afectadas de la CII.

A. Iniciativas y Aplicaciones Reales

Actualmente, existen varios estudios correspondientes a diversas áreas de investigación y aplicaciones concretas, siendo éstas simples, complejas o críticas, y funcionando en los diferentes sectores (agrícola, sanitario, militar, industrial, etc.). De hecho, algunos científicos consideran a este tipo de redes adecuados para monitorizar el estado físico de las infraestructuras civiles (puentes, túneles, tuberías, edificios o minas de carbón) para evitar terribles catástrofes, como el ocurrido en el puente I-35W del río Mississippi de los Estados Unidos, el cual fue construido en 1967 y presentaba considerables deficiencias en sus estructuras.

Efectivamente, los materiales de construcción de los puentes tienden a perder calidad con el tiempo, además de estar expuestos a cambios significativos del medio (vibraciones, presiones o cambios de temperatura), así que Uhl et. al. describieron en [8] una forma de monitorizar tales eventos mediante una red de sensores. Fraser et. al. [9] de la Universidad de California presentaron una forma de controlar el tráfico en puentes de 100 metros de largo mediante sensores y cámaras de video. Por otro lado, Kim et. al. [10] realizaron un profundo análisis sobre la posibilidad de controlar tales infraestructuras examinando las vibraciones existentes.

Otras de las CI son los túneles, minas, tuberías y subsuelos. De hecho, Cheekiralla [11] realizó un estudio en los túneles de Londres (LUL) para probar la viabilidad de las redes de sensores en túneles que se encuentran en proceso de restauración o en construcción. Mohanty propuso en [12] una aplicación para rastrear las actividades de los mineros y monitorizar las condiciones reales de las minas, y Chehri et. al. [13] presentaron un estudio sobre la necesidad de monitorizar las condiciones físicas de las minas. Igualmente, Stoianov en [14] expuso una forma de monitorizar el estado físico de las tuberías controlando sus vibraciones y el nivel de agua para determinar posibles brechas y fugas.

Sin embargo, éstos no son los únicos trabajos existentes, la Universidad de California [15] analizó los niveles de arsénicos en aguas subterráneas de Bangladesh desplegando una red de sensores bajo agua, además de analizar los niveles de nitrato del suelo. Beckwith et. al. [16] utilizaron las redes de sensores para mejorar la producción del vino. Sharp et. al. [17], en el sector militar, presentaron una forma de localizar un objeto e informar de su posición actual y Melloy [18] propuso un proyecto para mejorar el espacio de defensa militar obteniendo información en tiempo real.

Aparte de estos trabajos, hoy en día, existen multitud de proyectos (nacionales e internacionales) que intentan explotar las ventajas ofrecidas por estos tipos de redes, como puede ser: el proyecto VITUS [19], el proyecto Underground M3 and Smart Infrastructure (WINES II) [20], CoBIS [21], o SMEPP [22]. Igualmente, existen organizaciones específicas (como, *Common wealth Scientific and Industrial Research Organisation* (CSIRO) [23] o *Center for Sensed Critical Infrastructure Research* (CenSCIR) [24]) que están introduciendo las redes de sensores en aplicaciones industriales, con el objetivo de

monitorizar sus maquinarias y/o el medio de operación. Con lo cual, estas redes son también adecuadas para ser instaladas y configuradas en sistemas SCADA (*Supervisory Control and Data Acquisition Systems*) [25].

III. Líneas de Investigación

A. Seguridad en Redes de Sensores

La seguridad en las redes de sensores ha sido estudiada de forma extensiva por la comunidad científica, y aunque aún existen problemas de seguridad que deben ser resueltos (p. ej. manejo de nodos móviles, delegación de privilegios, privacidad, agentes seguros, actualización del código [26]), actualmente es posible crear una red de sensores que cumpla un conjunto básico de propiedades de seguridad. Para cumplir con ese conjunto mínimo de propiedades seguras en sus operaciones internas, las redes de sensores deben utilizar primitivas criptográficas, utilizar sistemas de gestión de claves, y proporcionar soporte para el conocimiento del entorno y la autoconfiguración.

Respecto a las primitivas criptográficas, el hardware actual de las redes de sensores es perfectamente capaz de soportar criptografía simétrica, criptografía de clave pública, y funciones hash. El estándar IEEE 802.15.4 proporciona soporte HW para ejecutar la primitiva AES-128, aunque ésta y otras primitivas pueden ejecutarse por SW. La implementación por SW de la primitiva AES-128 ocupa 8kB de ROM y 300 bytes de RAM [27]. Además, existen otros algoritmos de cifrado en bloque y cifrado en flujo como Skipjack [27] y RC4 [28] que, aunque más débiles, tienen unos requerimientos de memoria más asequibles: 2600 y 428 bytes de ROM, respectivamente.

Los nodos sensores han sido normalmente considerados como dispositivos demasiado restringidos para soportar criptografía de clave pública, pero esta suposición ha cambiado. Utilizando criptografía de curvas elípticas (ECC), es posible tener soporte para cifrar datos (ECIES), firmar y verificar (ECDSA), y negociar claves (ECDH) en un nodo sensor. De todas formas, los requerimientos computacionales y de memoria de estos algoritmos siguen siendo altos: una firma utilizando ECDSA consume aproximadamente 2 segundos, y el algoritmo ocupa 17kB de ROM y 1.5kB de RAM [29]. Finalmente, los nodos sensores pueden implementar funciones hash como SHA-1 en solo 3kB de ROM.

Al implementar ECDH en los nodos sensores, es posible resolver el problema de la distribución de claves en una red de sensores. Sin embargo, pueden existir escenarios en los que la funcionalidad de la aplicación sea tan compleja que los nodos sensores no tengan capacidad para implementar las primitivas de clave pública, o incluso que los requerimientos de la aplicación no necesiten de la complejidad de ECDH. La gestión de claves sigue siendo una línea de investigación abierta, aunque con el estado del arte actual es posible satisfacer los requerimientos de redes de sensores pequeñas [30].

La criptografía puede utilizarse como base para crear servicios de seguridad esenciales (confidencialidad, integridad, autenticación), pero estos servicios no son suficientes para cumplir una de las propiedades inherentes a las redes de sensores: la autoconfiguración. Para ser completamente autónomos y autosuficientes, los nodos sensores deben ser capaces de reconocer los eventos que ocurren en su entorno, y que pueden afectar al funcionamiento de la red. Actualmente, existen mecanismos de conocimiento del entorno que pueden detectar eventos anómalos dentro de una red de sensores [31]. Estos mecanismos pueden utilizarse tanto para controlar el estado de la red como para ofrecer soporte a los principales protocolos de una red de sensores: enrutado, agregación, y sincronización temporal.

B. Interoperabilidad

Como ya se ha mencionado en este artículo, las redes de sensores es una tecnología apropiada para CIIP. No obstante, integrar este tipo de tecnología en una CII no es una tarea sencilla, y menos aún, si se desea utilizar sistemas adicionales que provean servicios adecuados para la protección, como son EWS y DRS. De hecho, este problema está siendo actualmente tratado en el proyecto CRISIS (*Critical Information Infrastructures Security based on Internetworking Sensors*) [32], el cual deberá definir y diseñar los componentes software, localizados en los nodos sensores, para proveer los mecanismos básicos para la creación de servicios de seguridad. A su vez, estos componentes deberán permitir el despliegue de un sistema de control distribuido, los accesos a la información percibida, y los accesos a los correspondientes subsistemas adyacentes.

Por otro lado, será necesario especificar mecanismos para asegurar una apropiada interoperabilidad entre los diferentes componentes del sistema, estableciendo las bases de las redes de sensores como una arquitectura orientada a servicios (*Service Oriented Architecture* (SOA)). A su vez, esta arquitectura deberá garantizar un sistema de gestión de confianza, autentificación para autenticar a cada una de las partes involucradas de la red y los recursos implicados, y servicios de delegación. Estos servicios serán la base para proveer otros más complejos, como son la agregación, el intercambio seguro de información, y privacidad. Además, éstos deberán colaborar conjuntamente para ofrecer sistemas de control seguros, con el objetivo de proporcionar servicios de monitorización y mantenimiento, tales como EWS, DRS dinámica y las técnicas de auditoría y forenses.

Además, será necesario una especificación completa del middleware y de las políticas de seguridad e interfaces para el intercambio seguro de información, así como también, el diseño de aquellos mecanismos que permitan una correcta intereoperabilidad entre los diferentes servicios (ya sean externos o internos de la red). Finalmente, será necesario desarrollar una herramienta de evaluación que permita verificar la seguridad de las interconexiones de los distintos sistemas en la CII, permitiendo (si es posible) crear un sistema de soporte de decisión. Dicho sistema, podrá identificar la estabilidad de las CII bajo un cierto contexto en base a propiedades de los nodos individuales, el sistema y su contexto, fallos e intrusiones para los cuales el sistema es susceptible.

IV. Conclusiones

Como se ha podido observar, existen numerosas aplicaciones reales y estudios donde la redes de sensores son las principales protagonistas en la CIP. Este artículo analiza su utilidad para esta misión. La importancia de esta investigación viene dada por la mayor relevancia que va adquiriendo CIIP tanto a nivel Español como a nivel mundial. Precisamente, el gobierno de España ha aprobado recientemente el Centro Nacional de Protección de Infraestructuras Críticas, donde uno de sus primeros objetivos será proteger los embalses y redes distribuidas de aguas, así como también, centrales eléctricas y de energía, el sector sanitario y alimenticio, transporte, y demás CI.

Dentro de las posibles mejoras y líneas de investigación a seguir, sería necesario optimizar las restricciones presentes en los nodos sensores, y explotar las características inherentes de las redes de sensores interactuando en colaboración con otros dispositivos de control (RFID, cámaras de videos, etc.). El camino es largo, pero no está exento de posibilidades, tal y como se ha visto en la sección II-A.

Agradecimientos

Este trabajo ha sido cofinanciado por los proyectos de investigación SMEPP (EU-FP6-IST 0333563) y CRISIS (TIN2006-09242). El trabajo de la autora Cristina Alcaraz ha sido financiado por el Ministerio de Educación y Ciencia Español (MEC), bajo el programa de formación de personal investigador. El trabajo del autor Rodrigo Román también ha sido financiado por el MEC, bajo el programa de formación de profesorado universitario.

References

[1] Critical Information Infrastructure Research Co-ordination (CI2RCO). *Deliverable D12, "ICT R&D for CIIP: Towards a European Research Agenda"*. 13 Abril 2007.

[2] National Research Council, L. Dahms. *Infrastructure for the 21st century - framework for a research agenda*. National Academy Press, Washington, D.C., 1987.

[3] President's Commission on Critical Infrastructure Protection (PCCIP). *Critical Foundations: Protecting America's Infrastructures*. Washington D.C., 1997.

[4] M. Dunn. *Threat Frames in the US Cyber-Terror Discourse*. Proceedings of the 2004 British International Studies Association (BISA) Conference, Warwick, 2004.

[5] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci (2002). *Wireless sensor networks: a survey*. Computer Networks: The International Journal of Computer and Telecommunications Networking, vol. 38, no. 4, pp. 393-422, Marzo 2002.

[6] D. Bopping, *CIIP in Australia*, 1st CI2RCO Critical Information Infrastructure Protection conference, Rome, Marzo 2006.

[7] Distributed Robotics Lab, http://groups.csail.mit.edu/drl/wiki/index.php/Main_Page, 2006.

[8] T. Uhl, A. Hanc, K. Tworkowski, and T. Sekiewicz, *Wireless sensor network based bridge monitoring system*, Key Engineering Materials Vol. 34, pp. 499-504, 2007.

[9] M. Fraser, A. Elgamal, L. Yan, and J. P. Conte, *Video and Motion Sensor-Network for Bridge Monitoring Applications*, 4th World Conference on Structural Control and Monitoring (WCSCM), pp. 11-16, Julio 2006.

[10] S. Kim, S. Pakzad, D. Culler, J. Demmel, G. Fenves, S. Glaser, and M. Turon, *Health monitoring of civil infrastructures using wireless sensor networks*, IPSN '07: Proceedings of the 6th international conference on Information processing in sensor networks, pp. 254–263, 2007.

[11] S. Cheekiralla, *Poster Abstract:Wireless Sensor NetworkBased Tunnel Monitoring*, Real-World Wireless Sensor Networks (REALWSN'05),Stockholm, Sweden, pp. 20–21 Junio 2005.

[12] P. Mohanty, *Application of Wireless Sensor Network Technology for Mziner Tracking and Monitoring Hazardous Conditions in Underground Mines*, A FI Response (MSHA RIN 1219-AB44), 2006.

[13] A. Chehri, P. Fortier, and P. Tardif, *Security Monitoring Using Wireless Sensor Networks*, CNSR '07: Proceedings of the Fifth Annual Conference on Communication Networks and Services Research, pp. 13–17, 2007.

[14] I. Stoianov, L. Nachman, S. Madden, and T. Tokmouline, *PIPENET: A Wireless Sensor Network for Pipeline Monitoring*, in IPSN'07, 2007.

[15] N. Ramanathan, L. Balzano, D. Estrin, M. Hansen, T. Harmon, J. Jay, W.J. Kaiser, G. Sukhatme, *Designing Wireless Sensor Networks as a Shared Resource for Sustainable Development*, in: Proceedings of the International Conference on Information and Communication Technologies and Development (ICTD 2006), Berkeley, USA, 2006.

[16] R. Beckwith, D. Teibel, P. Bowen, *Report from the field: Results from an agricultural wireless sensor network*, in Proceedings of the 1st IEEE Workshop on Embedded Networked Sensors (EmNetS-I 2004), Tampa, USA, Noviembre 2004.

[17] C. Sharp, S. Schaffert, A. Woo, N. Sastry, C. Karlof, S. Sastry, D. Culler, *Design and Implementation of a Sensor Network System for Vehicle Tracking and Autonomous Interception*, in Proceedings of the 2nd European Workshop on Wireless Sensor Networks (EWSN 2005), pp. 93–107, Istanbul, Turkey, Enero 2005.

[18] J. Melloy, *Wireless Sensor Network Applications for the Combat Air Forces*, Graduate research project, Airforce Institute of Technology. Junio 2006.

[19] Schwabach, H., Harrer, M., Waltl, A., Horst, B., Tacke, A., Zoffmann, G., Beleznai, C., Strobl, B., Helmut, G., Fernández, G., *VITUS: Video based Image analysis for Tunnel Safety*. In: International Conference on Tunnel Safety and Ventilation, 2006.

[20] WINES II – Smart Infrastructure University of Cambridge and Imperial College, London, http://www.winesinfrastructure.org, 2006.

[21] CoBIS: *Collaborative Business Items project*, http://www.cobis-online.de, 2004–2007.

[22] SMEPP: *Secure Middleware for Embedded Peer-to-Peer Systems*, FP6-2005-IST-5, http://www.smepp.org, 2006.

[23] G. Platt, M. Blyde, S. Curtin, and J. Ward, *Distributed wireless sensor networks and industrial control systems - a new partnership*, EmNets '05: Proceedings of the 2nd IEEE workshop on Embedded Networked Sensors, 157–158 pp, 2005.

[24] Center for Sensed Critical Infrastructure Research (CenSCIR), http://www.ices.cmu.edu/censcir/, 2006.

[25] L. Piè andtre-Cambacé anddè ands,P.Sitbon, *Cryptographic Key Management for SCADA Systems-Issues and Perspectives*, International Conference on Information Security and Assurance (ISA 2008), pp. 156-161, 2008.

[26] J.P. Walters, Z. Liang, W. Shi, V. Chaudhary. *Wireless Sensor Network Security: A Survey*, Security in Distributed, Grid, and Pervasive Computing, Ed. Y. Xiao, CRC Press, 2006.

[27] Y.W. Law, J. Doumen, P. Hartel. *Survey and Benchmark of Block Ciphers for Wireless Sensor Networks*, ACM Transactions on Sensor Networks, Vol. 2, No. 1, pp 65-93, 2006.

[28] K.J. Choi, J.-I. Song. *Investigation of feasible cryptographic algorithms for wireless sensor network*, Proceedings of the 8th International Conference on Advanced Communication Technology (ICACT 2006), Phoenix Park, Corea del Sur, pp. 1379-1381, 2006.

[29] A. Liu, P. Ning. *TinyECC: A Configurable Library for Elliptic Curve Cryptography in Wireless Sensor Networks*. Technical Report TR-2007-36, North Carolina State University, Department of Computer Science, Noviembre 2007.

[30] C. Alcaraz. (2008). *KMS CRISIS Guidelines Web Application*. http://www.isac.uma.es/CRISIS/tools.html.

[31] R. Roman, J. Lopez, S. Gritzalis. *Situation Awareness Mechanisms for Wireless Sensor Networks*. IEEE Communications Magazine. Vol. 46, No. 4, pp 102-107, 2008.

[32] CRISIS: *CRitical Information Infrastructures Security based on Internetworking Sensors*, http://www.isac.uma.es/CRISIS/, TIN2006-09242, Proyecto Español MEC I+D, 2006–2009.