C. Alcaraz, and J. Lopez, "Análisis de Seguridad de las Redes Mesh de Sensores en Sistemas Críticos de Control", *VIII Jornadas de Ingeniería Telemática (JITEL09)*, pp. 483-486, 2009.
NICS Lab. Publications: https://www.nics.uma.es/publications

Análisis de Seguridad de las Redes Mesh de Sensores en Sistemas Críticos de Control

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

***Resumen*—Los sistemas críticos de control representan un componente fundamental para el correcto funcionamiento de muchas de las infraestructuras críticas existentes en nuestra sociedad. Actualmente, estos sistemas incluyen en su diseño infraestructuras y tecnologías de última generación para mejorar los procesos de control, como por ejemplo las redes de sensores. Por ello, varios organismos internacionales están trabajando activamente con el objeto de estandarizar las comunicaciones a este nivel, así como para garantizar la conservación de energía de sus nodos, la coexistencia con las demás redes, y la fiabilidad y seguridad de tales comunicaciones. Desafortunadamente, y tal y como se pone de relieve en este artículo, la seguridad no está totalmente garantizada dado que existen diversas vulnerabilidades asociadas, que ponen en riesgo la funcionalidad general del sistema. En este artículo se realiza un análisis pormenorizado a este respecto, estableciendo además un conjunto de recomendaciones y consideraciones con el fin de mejorar tales especificaciones en los mencionados esfuerzos de estandarización.**

***Palabras Clave*—Sistemas Críticos de Control Críticos, Sistemas SCADA, Redes Mesh Inalámbrica de Sensores.**

I. Introducción

Los sistemas SCADA actuales hacen uso de múltiples y diversas tecnologías para favorecer los procesos de monitorización. De hecho, una de las tecnologías por la que la industria está apostando es la comunicación inalámbrica ya que garantiza los mismos servicios de control que una cableada a un bajo coste de instalación y mantenimiento. Siguiendo en esta misma línea, las *Redes Inalámbricas de Sensores* son también objeto de interés, al proveer atractivos servicios para el control. Es por ello que diversos organismos internacionales están dedicando un esfuerzo nada desdeñable a la estandarización de sus respectivas comunicaciones.

Debido a la criticidad de los sistemas de control y de los sistemas monitorizados, es necesario analizar todos los posibles ataques asociados a estos estándares de comunicación, y asegurar seguridad de los datos críticos, disponibilidad de recursos y protección de ciertos servicios de operación, tal como: comandos/órdenes o lecturas/alarmas. Además, en este tipo de análisis entra en juego el contexto de aplicación, las acciones intencionadas de los propios miembros de la organización y de los miembros ajenos a ésta. Como resultado, un conjunto de recomnedaciones se han propuesto para mejorar sus especificaciones y mitigar cualquier tipo de efecto en cascada sobre el sistema monitorizado.

El artículo está organizado en cinco secciones: la sección II introduce el concepto de sistema crítico de control y presenta la tecnología de las redes de sensores para el control de las infraestructuras críticas. En la sección III se introducen los estándares de comunicación, profundizando en la seguridad de los mismos, que pasa a ser analizada y discutida en la sección IV. Finalmente, en la sección V se encuentran las conclusiones y trabajo futuro.

II. Sistemas SCADA y tecnologías

Un sistema SCADA [1] es un sistema de control cuya labor es la de monitorizar otras infraestructuras críticas pertenecientes principalmente al sector industrial. Las características implícitas y críticas de estos sistemas hacen que un sistema SCADA requiera funcionalidad del sistema, disponibilidad de sus recursos y, sobre todo, seguridad dado que son muy vulnerables a multitud de ataques, la mayoría derivados de acciones maliciosas o negligentes.

El núcleo principal de estos sistemas lo forma el "Centro de Control", en el que los operarios pueden conocer en tiempo real el estado de las infraestructuras monitorizadas simplemente observando datos o alarmas recibidas por las subestaciones remotas instaladas de manera jerárquica en todo el área. La gestión de estas subestaciones se puede realizar desde cualquier localización geográfica y a través de diversas infraestructuras de comunicación, como puede ser la inalámbrica. De hecho, varias organizaciones ([2], [3], [4]) están trabajando activamente en la estandarización de éstas, las cuales contemplan a su vez las redes de sensores [5] como un perfecto elemento de control. Este hecho se debe principalmente por las características inherentes de sus nodos sensores, cuyas mediciones se corresponden con las condiciones físicas y reales de las infraestructuras monitorizadas. Obviamente, una red de sensores en un sistema SCADA debe enviar tales datos al centro de control para que los operarios puedan ser capaces de interpretarlos. De forma similar, estas redes pueden ofrecer a los operarios ciertos servicios de consulta en tiempo real, detectar situaciones anómalas y generar alarmas con el fin de resolver el problema dentro de un periodo de tiempo límite. Asimismo, los nodos sensores pueden ofrecer autonomía, independencia y auto-configuración para funcionar en cualquier área de desarrollo y en cualquier contexto de aplicación.

Sin embargo, distribuir una red de sensores como parte esencial de un sistema de control supone tener en cuenta algunos aspectos relacionados con la conservación de energía, fiabilidad de las comunicaciones al existir una alta probabilidad de interferencias industrial, coexistencia con otras redes de comunicación, restricciones hardware y softwarre, y por supuesto seguridad. Con respecto a este último, es importante comentar que existen algunos avances en la utilización de primitivas criptográficas (de clave simétrica y pública), funciones hash, y mecanismos de negociación y distribución de

claves [6].

III. Estándares de Comunicación y su Seguridad

Los estándares ZigBee PRO [4], WirelessHart [7] e ISA100.11a [8] están basados de IEEE 802.15.4-2006 [9], cuyos nodos tramisten a baja frecuencia y tienen limitadas capacidades hardware y software, así como también de energía. Sus dispositivos pueden funcionar a 2.4GHz a 250 kbps o 868-915MHz a 20 kbps, con 15 canales de transmisión, y cuya capa de enlace controla los accesos al medio mediante CSMA-CA. Además, provee soporte para AES-128bits y gestiona una lista de control de acceso (ACL, *Access Control List*), donde se mantiene el ID del nodo a comunicar, la política de seguridad a utilizar, una clave de 128 bits, un vector inicial y un contador. En el caso de que el nodo no esté en dicha lista, su mensaje debe ser rechazado o tiene que pasar otros mecanismos de autentificación.

A. ZigBee PRO

ZigBee PRO, especificada en ZigBee-2007, tiene como objetivo proporcionar coexistencia y control en redes de comunicación mesh y redes de muchos-a-uno. Su arquitectura de red está basada en tres nodos principales: un gateway (entidad de mayor confianza), routers y los nodos sensor finales. Dicha red provee varios servicios, como son: un "gestor de enlace asimétrico" para configurar aquella ruta con mejor calidad simétrica entre pares de nodos, "agilidad de la frecuencia" para analizar las interferencias u obstáculos en canal y cambiar de canal si hace falta, "rutas compartidas de muchos-a-uno" donde se mantiene una tabla de enrutamiento con una única entrada hacia el gateway, y "enrutamiento origen" para recordar la ruta de vuelta desde el gateway al nodo origen. También, se controla los conflictos de identidad mediante el uso de "direccionamiento estocástico", donde apriori se asigna a cada nodo nuevo una dirección aleatoria y en caso de conflicto activar un mecanismo de resolución de identidades. Por último, ZigBee PRO provee dos modos de seguridad: "seguridad estándar" y "seguridad alta", y ambas son mantenidas por el gateway.

En el modo de "seguridad estándar" se manejan dos claves: clave de enlace (Cenl) y de red (Cred). La Cenl (única y opcional) es compartida entre pares de nodos, y es usada para cifrar los mensajes en la capa de aplicación. En cambio, la Cred es una clave usada para cifrar las comunicaciones a nivel de red y es compartida por todos los dispositivos del sistema. Esta clave puede ser actualizada por el gateway a través de un mensaje en difusión cifrada con la antigua Cred. Cuando un nodo se une a la red puede adquirir la Cred de dos maneras, bien haciendo uso de la Cenl preconfigurada en el nodo para cifrar la Cred, o bien, recibirla desde el gateway en claro. Obviamente, este último caso no es muy aconsejable en entornos críticos.

En cambio, en el modo de "seguridad alta" se incluye una clave más al conjunto anterior: la clave maestra (Cmaestra). Esta clave es preconfigurada en el nodo para generar la Cenl aplicando el algoritmo Symmetric-Key Key Exchange (SKKE). Una vez generada la Cenl, el gateway transmite la Cred cifrada con la Cenl al nodo correspondiente. Esta clave de red es actualizada de manera periódica, incluso cuando los nodos son excluidos de la red. El principal problema asociado a este modo es la alta sobrecarga de memoria, sin embargo, esto garantiza seguridad en aplicaciones críticas.

B. WirelessHart

WirelessHart, especificado como parte de [10], define un protocolo de red mesh para el control de automatización industrial manteniendo máxima compatibilidad con las tecnologías ya existentes de HART. Su arquitectura de red está compuesta de nodos sensores adheridos a dispositivos de campo, dispositivos portables (PDAs, móviles, etc.), gateways para la interconexión entre sistemas de comunicación y un gestor de red. Dicho gestor, el cual podría estar integrado en el propio gateway, establece la configuración de red y define las tablas de enrutamiento de los nodos, así como también, planifica las comunicaciones entre dispositivos.

Su capa capa física está bajo [9], sin embargo, éste define su propia capa de enlace estableciendo tiempos fijos de sincronización mediante TDMA/CSMA. Controla las altas interferencias en los canales de comunicación aplicando los métodos "blacklisting" (incluir en una lista aquellos canales con alto índice de ruido) y "hopping" (cambiar de canal de radio frecuencia). Con respecto al enrutamiento de mensajes, el propio gestor de red establece las diversas rutas redundantes asociadas a un nodo de la red. La actualización de dichas tablas se realiza por cada nueva integración y se procede en todos los nodos de red involucrados en la comunicación. También, WirelessHart ofrece seguridad tanto a nivel de enlace como a nivel de red. En ambos, se hace uso de cuatro tipos de claves diferentes: clave pública (Cpub), usada para generar en la fase de despliegue el código de integridad de mensajes (MIC) de la capa de enlace. Clave de red (Cred), compartida por todos los dispositivos y utilizada para generar el MIC en la capa de enlace. Clave de unión (Cunión), única para cada nueva integración y es usada para generar el MIC en la capa de red y para cifrar el mensaje de nueva unión. Clave de sesión (Csesión), única entre un nodo de la red y el gestor de red, y es utilizada para cifrar los mensajes. En lo que respecta a la generación del MIC, ésta está basada en el modo CCM* junto con AES-128bits y tomando como parámetros: la cabecera del paquete sin cifrar y su cuerpo, una clave de 16 bytes (Cpub si el nodo es nuevo o Cred si ya existe) y un nounce único de 13 bytes.

Antes de que un nodo nuevo se integre en la red, éste debe ser preconfigurado con la ID de la subred a la que tiene que unirse, la Cpub y la Cunión. Cuando el nodo es posicionado en la red, éste debe hacerse conocer públicamente mediante un mensaje de nueva unión, junto con el MIC de la capa de enlace cifrado con la Cpub y el MIC de la capa de red cifrado con la Cunión. Una vez que este mensaje es recibido por el gestor de red, éste lo autentifica con su clave privada y genera una Csesión única. Tras la generación, el gestor trasmite la Csesión y la Cred a la nueva incorporación cifrado con la Cunión. En paralelo, el gestor prepara la nueva planificación y la tabla de enrutamiento, y ambas, son transmitidas a todos los nodos de la red. En el caso de que un nodo sensor ya existente en la red desee enviar datos al gestor de red, éste deberá autentificarse con la Cred y el paquete es cifrado con la Csesión. Por último, es importante comentar que todas estas claves no son actualizadas durante toda la vida útil de un nodo sensor (entre 5 y 10 años) [11].

C. ISA100.11.a

ISA100.11.a es un estándar recientemente validado y está pensado para ser un estándar abierto. Su especificación está planteada para ser funcional en redes mesh o en estrella cuyos nodos son baja complejidad. Está enfocado para ser aplicados en aplicaciones industriales, garantizando conservación de energía, escalabilidad, interoperabilidad, fiabilidad en las comunicaciones y seguridad. Como puntualización, al no encontrarse este estándar aún disponible, no se ha sido posible realizar el estudio de seguridad.

IV. Análisis de Seguridad de ZigBee PRO y WirelessHart

Considerando como taxonomía base de amenazas la propuesta por Tsao et al. en [12], varios ataques han sido identificados en los respectivos estándares.

A. Amenazas Zigbee PRO

Debido al contexto crítico de los sistemas de control, el análisis se enfocará sobre el modo de "seguridad alta". De hecho, varios ataques contra la confidencialidad han sido ya identificados, como por ejemplo: *exposición deliberada* y *control de acceso remoto*, donde un operador del sistema conoce y preinstala la Cmaestra en un nodo sensor para pasar los mecanismos de autentificación en el gateway y unirse a la red como si éste fuese un nuevo nodo legítimo. Similarmente, existe ataque de *escucha del canal* cuando un operador conoce la Cmaestra y es capaz de interpretar las transacciones de SKKE entre dos nodos de la red con el fin de generar la Cenl de ambos. En dicho momento, el adversio puede tener la capacidad de deducir la Cred, y por lo tanto, leer cualquier mensaje en el canal. Además, un malicioso miembro ajeno de la organización podría ser también capaz de deducir la Cenl observando el contenido de los mensajes, por lo que se recomienda actualizarla de manera frecuente. Además, para mitigar los tres ataques anteriores sería conveniente establecer rigurosas políticas de seguridad, llevar a cabo regulares auditorías (p. ej. NIST SP800-53 revisión 2) y hacer uso de mecanismos de autentificación.

Un adversario es capaz también de deducir la topología de la red simplemente observando el tráfico de la red, el cual va dirigido siempre hacia el gateway. Este hecho podría capacitar al adversario a aproximarse a la localización física del gateway para realizar otros ataques futuros. Una solución sería mantener una tabla con varias entradas, sin embargo, esto no es factible, ya que las tablas tienen una sóla entrada. Por consiguiente, sería necesario actualizar dichas tablas de manera periódica. Con respecto a los *ataques físicos*, éstos dependerán del tipo de protección del área de trabajo y del tipo de acceso a la misma. Lo ideal sería configurar mecanismos de protección en todo el perímetro de distribución haciendo uso de procedimientos de autentificación para el acceso, así como el uso cámaras de video vigilancia. Por otro lado, es necesario seguir avanzando en el diseño de la plataforma hardware de los nodos para que sean resistentes frente ataques físicos.

No existe ataque de *manipulación de datos* al transmitirse el MIC junto con el mensaje cifrado. Tampoco existe ataque de *reenvío de mensajes* al utilizarse un contador único en cada envío. Sin embargo, y aunque no exista ningún nodo específico que reconfigure las tablas de enrutamiento, existe la posibilidad de que varios nodos maliciosos en la red puedan mentir sobre la calidad de sus rutas en el momento de determinar cúal es la ruta con mejor calidad simétrica al gestor de enlace asimétrico. Luego, existe ataque de *falsificación de rutas*. También, puede existir ataque *sybil* cuando la clave Cenl entre dos nodos es deducida por haber comprometido la Cmaestra, por lo que se recomienda realizar periódicas actualizaciones de ésta. Por el contrario, no existen ataques *sinkhole* y *wormhole* al gestionarse una ACL con todos los vecinos de confianza. En cambio, los ataques de *inundación* de paquetes y de *reenvío selectivo* son controlados al gestionarse tablas de enrutamiento de una sóla entrada, y por lo tanto, un sólo nodo vecino deberá recibir el mensaje. Tampoco existe sobrecarga del canal y *obstrucción del medio* al utilizarse la técnica de agilidad de frecuencia.

Existe ataque *blackhole* cuando un nodo supuestamente legítimo de la red no reenvía los mensajes. Es posible mitigar este ataque enviando el mensaje por varias rutas a la vez o seleccionando dinámicamente el siguiente nodo de entre un conjunto de candidatos. Sin embargo, estas soluciones entran en conflicto con la propia definición del protocolo, por lo que se deberá tener en cuenta para mejorar su especificación. También, es posible *aislar la red* cuando el gestor de enlace asimétrico recibe datos falsos de los nodos vecinos que mienten sobre la calidad de su enlace para anular todas las posibles rutas a tomar. Esto supone que la mayoría de nodos de la red, y al menos uno en cada ruta, están comprometidos. Lo cual puede ser resuelto mediante frecuentes procesos de mantenimiento y de inspección de la red.

B. Amenazas en WirelessHart

En WirelessHart pueden existir varios tipos de amenazas, como: *exposición deliberada* y *control de acceso remoto* donde un operador quiere ganar ciertos accesos al sistema preinstalando la Cpub y Cunión en un nodo supuestamente legítimo de la red. Por ello, es necesario implantar fuertes políticas de seguridad, que incluyan rigurosos mecanismos y procedimientos de autentificación y auditoría. Por otro lado, como no se cifra al completo los mensajes intercambiados en el canal de comunicaciones y la actualización de las tablas de enrutamiento de los nodos dependen de la frecuencia de unión de nuevos nodos a la red, puede existir un ataque de *análisis del tráfico*. Una solución sería actualizar periódicamente las tablas de enrutamiento sin que ello suponga esperar nuevas y futuras (quizás lejanas) incorporaciones. También, existe posibilidad de que se lleve a cabo un *ataque físico* si el área de desarrollo es fácilmente accesible o está totalmente desprotegida, por lo que se recomienda securizar el medio y proteger la estructura hardware de los nodos. Igualmente, un adversario puede ser capaz de deducir las credenciales de seguridad de un nodo sensor al no requerirse frecuentes actualizaciones de éstas durante toda su vida útil. Por lo que si un atacante deduce las Csesión entre un nodo y el gestor de red, éste es capaz de leer el contenido de todos los mensajes cifrados con dicha clave. Obviamente, la solución sería actualizar las credeciales de seguridad de manera periódica.

Aunque no existe ataque de *manipulación de datos críticos* por enviar los mensajes junto con el MIC generado con la Cred, existe ataque de *falsificación de rutas* cuando el gestor de red es comprometido por algún miembro de la organización

con determinados accesos al sistema. Una forma de evitar este ataque es securizando todos los puntos de accesos al sistema SCADA y aprovechar las capacidades hardware y software del gestor para configurar mecanismos de autentificación potentes, además de realizar frecuentes procedimientos de auditorías. Por el contrario, no existe ataque *sybil* durante el proceso de únion al autentificarse con la Cpub. Sin embargo, si es posible realizar ataques sybil cuando la Csesión entre un nodo y el gestor es comprometida. Para mitigar este ataque lo ideal sería realizar frecuentes actualizaciones de la Csesión y que el propio gestor de red sea capaz de controlar la recepción de los mensajes de una supuesta y misma identidad.

No existe ataque de *reenvíos de mensajes*, ya que se usa un nounce de 13 bytes para la generación del MIC. Asimismo, no existe ataque de *obstrucción del medio* al utilizarse la técnica hopping y el uso de rutas redundantes. Tampoco existe ataque de *inundación* de paquetes al establecerse rutas concretas hacia el gestor de red. Por el contrario, existe ataque *reenvío selectivo* al mantenerse una tabla de enrutamiento con rutas redundantes, por lo que sería conveniente enviar dicho mensaje por varias rutas diferentes. También, existe ataque *blackhole* cuando un nodo supuestamente legítimo de la red recibe datos y no los reenvía al nodo siguiente de la tabla de enrutamiento. Para evitar dicho ataque es necesario modificar directamente la definición del protocolo para permitir el envío de paquetes por múltiples rutas o mediante una selección dinámica del siguiente nodo.

Puede existir un ataque *sinkhole* y *wormhole* cuando un nodo (o varios) de la red transmite información falsa al gestor de la red para modelar las tablas de enrutamiento a su beneficio. Esto se puede evitar estableciendo una política de aislamiento de nodos maliciosos usando un umbral específico sobre la cantidad de tráfico o recibir la información sólo del nodo vecino fiable mediante el uso de algún mecanismo de confianza. Igualmente, pueden surgir *aislamientos de la red* cuando ciertos ataques de denegación de servicios aparecen en la interfaz entre el centro de control y la red de sensores. En este caso un operador malicioso podría sobrecargar al gateway con múltiples órdenes/comandos mediante el uso de algún protocolo SCADA (p.ej. Modbus/TCP [13]). Una forma de evitarlo sería implementar mecanismos automatizados e inteligentes que gestionen la frecuencia de envío por operador favorenciendo los procesos de auditorías futuros. Otra forma de aislar la red se consigue generando altas interferencias en el canal con el fin de bloquear los 15 canales de frecuencias. Este hecho incapacita a los nodos a transmitir por ningún canal. En este caso, se aconseja monitorizar el medio de distribución para conocer el origen del fenómeno que genera las interferencias y quitar de la lista blacklisting todos aquellos canales ya disponibles.

V. Conclusiones y Trabajo Futuro

El proposito de este artículo ha sido realizar un profundo análisis de seguridad de los estándares de comunicación inalámbricos aprobados recientemente, donde es posible observar en la tabla I que la mayoría de los ataques son generalmente originados por los propios (ex-)miembros del sistema. Bajo estas condiciones, se recomienda actualizar las tablas de enrutamiento y credenciales de seguridad, no sólo frecuentemente, sino cuando un operador abandona (temporalmente o definitivamente) la organización. Igualmente, se hace necesario diseñar e implementar mecanismos automatizados e inteligentes capaces de explorar todas las actividades desarrolladas, así como también, establecer rigurosas políticas de seguridad, y realizar frecuentes auditorías y mantenimiento. Todas estas recomendaciones y muchas otras han sido comentadas a lo largo de este artículo. Por último, es importante comentar que el análisis de seguridad de ISA100.11.a se ha propuesto como trabajo futuro al no estar aún disponible.

Tipos de Ataques	ZigBee PRO		WirelessHart	
Exposición Deliberada	✓	I	✓	I
Escucha del canal	✓	A	✓	A
Análisis del Tráfico	✓	A	✓	A
Acceso y Control Remoto	✓	I	✓	I
Ataque Físico	✓	A	✓	A
Manipulación de Datos Críticos	x	-	x	-
Falsificación de Rutas	✓	I	✓	I
Reenvío de Mensajes	x	-	x	-
Inundación	x	-	x	-
Reenvío Selectivo	x	-	✓	I
Blackhole	✓	I	✓	I
Sybil	✓	A	✓	A
Sinkhole	x	-	✓	I
Wormhole	x	-	✓	I
Obstrucción del Medio	-	x	-	x
Aislamiento de la Red	✓	I	✓	I

Tabla I
Análisis de Seguridad de ZigBee PRO y WirelessHart. Miembro del sistema (I), miembro ajeno (E) y ambos (A)

Agradecimientos

Este trabajo ha sido financiado por CRISIS (TIN2006-09242) y ARES (CSD2007-00004), agradeciendo a Rodrigo Román sus constructivos comentarios.

Referencias

[1] C. Alcaraz, G. Fernández, R. Román, A. Balastegui, J. López, "Secure Management of SCADA Networks", New Trends in Network Management, CEPIS, vol. IX, no. 6, pp 22-28, 2008.

[2] ISA100 "Wireless Systems for Automation", http://www.isa.org/Content/NavigationMenu/Technical_Information/ASCI/ISA100_Wireless_Compliance_Institute/ISA100_Wireless_Compliance_Institute.htm, 2009.

[3] HART Communication, http://www.hartcomm2.org, 2009.

[4] ZigBee Alliance, http://www.zigbee.org/, 2009.

[5] J. Yick, B. Mukherjee, D. Ghosal, "Wireless sensor network survey", Computer Networks Journal, vol 52, num 12, pp 2292–2330, Elsevier, 2008.

[6] R. Roman, C. Alcaraz, N. Sklavos. "On the Hardware Implementation Efficiency of Criptographic Primitives", Cryptology and Information Security Series, vol 1, pp 285–305, 2008.

[7] S. Jianping, H. Song, K. Mok,C. Deji, M. Lucas, M. Nixon, "WirelessHART: Applying Wireless Technology in Real-Time Industrial Process Control", RTAS apos'08, vol 22, num 24, pp 377–386, 2008.

[8] ISA100.11a, http://www.isa.org/MSTemplate.cfm?MicrositeID=1134&CommitteeID=6891, 2009.

[9] IEEE 802.15.4-2006, http://standards.ieee.org/getieee802/download/802.15.4-2006.pdf, 2006–2009.

[10] HART Communication Foundation, http://www.hartcomm2.org/hart_protocol/wireless_hart/hart7_overview.html, 1993–2009.

[11] D. Nilsson, T. Roosta, U. Lindqvist, A. Valdes, "Key management and secure software updates in wireless process control environments", WiSec'08, pp 100–108, ACM, 2008.

[12] T. Tsao, R. Alexander, M. Dohler, V. Daza, A. Lozano, "A Security Framework for Routing over Low Power and Lossy Networks", http://tools.ietf.org/id/draft-tsao-roll-security-framework-00.txt, 2009.

[13] Modbus-IDA. "The Architecture for Distributed Automation", http://www.modbus.org/, 2005–2009.