Un Enfoque Tolerante a Interrupciones para la Seguridad de la Internet de las Cosas

Daniel Ezquerra, Àngela Fabregas, MCarmen de Toro, Joan Borrell
Depto. de Ingeniería de la Información y de las Comunicaciones
Universitat Autònoma de Barcelona - Escola d'Enginyeria - Edifici Q
08193 Bellaterra, Spain
Email: {daniel.ezquerra,angela.fabregues,mcarmen.detoro,joan.borrell}@deic.uab.cat

***Resumen*—La Internet de las cosas (IoT, *Internet of Things*) es un paradigma emergente que pretende la interconexión de cualquier objeto susceptible de contar con una parte de electrónica, favorecido por la miniaturización de los componentes. El estado de desarrollo de la IoT hace que no haya ninguna propuesta firme para garantizar la seguridad y la comunicación extremo a extremo. En este artículo presentamos un trabajo en progreso hacia una aproximación tolerante a retrasos (DTN, *Delay and Disruption Tolerant Networks*) para la comunicación en el paradigma de la IoT y planteamos la adaptación de los mecanismo de seguridad existentes en DTN a la IoT.**

***Palabras clave*—Internet of Things(IoT), Redes tolerantes a retrasos e interrupciones(DTN), Seguridad en IoT.**

I. Introducción

La evolución de la tecnología ha permitido la miniaturización de muchos componentes electrónicos y junto con esta miniaturización ha aparecido la posibilidad de interconectar millones de dispositivos. Mientras que hasta ahora la mayoría de dispositivos interconectados eran controlados por humanos, esta evolución permitirá la comunicación máquina a máquina u objeto a objeto, con el fin de cooperar y lograr objetivos comunes. Es esta la idea que define la Internet de las cosas (IoT, *Internet of Things*) [1] y la Internet de las nano-cosas (IoNT, *Internet of Nano-Things*) [2], nuevos paradigmas en el escenario de las redes no cableadas.

Si consideramos la comunicación entre cualquier tipo de objeto, más allá de la comunicación entre ordenadores personales o teléfonos inteligentes, encontramos que el número de objetos conectados podría superar los 100 billones [3]. Si además consideramos los nano dispositivos podemos encontrarnos en un escenario donde se podría producir una monitorización constante de datos sensibles, como datos referentes a la salud (constantes vitales de un usuario) o las posiciones geográficas. Esta es la razón por la cual, antes de que la IoT pueda ser ampliamente aceptada, es el momento de trabajar en la seguridad de este paradigma.

Existe un gran número de propuestas que intentan definir los límites de lo que debe ser la IoT y cuales deben ser los bloques que la conformen. Asimismo se trata de definir los estándares y las visiones que serán ampliamente aceptadas en este nuevo paradigma. Igual pasa en otros paradigmas emergentes, como es el caso de la arquitectura de red tolerante a retrasos (DTN, *Delay and Disruption Tolerant Networks*)[4], dónde están apareciendo trabajos que tratan de dar respuesta a necesidades de seguridad y comunicación.

En este artículo presentamos un trabajo en progreso hacia una aproximación a la seguridad de la IoT mediante un un enfoque tolerante a interrupciones y retrasos basado en DTN.

La arquitectura DTN está pensada para escenarios con grandes retrasos, donde no es posible la comunicación extremo a extremo y donde existen una gran variedad de dispositivos. Debido a su diseño, la DTN es una arquitectura que podría resultar adecuada para dar respuesta a las necesidades comunicativas de la IoT. Al mismo tiempo, diversas soluciones de seguridad han sido estudiadas para cubrir las necesidades de la arquitectura DTN. Debido a la similitud entre las necesidades de las DTN y las necesidades de la IoT, creemos que las medidas de seguridad con validez en el campo de las DTN podrían ser adaptadas para usarse en la IoT.

El resto del artículo está estructurado de la siguiente manera: en la segunda sección presentamos el trabajo previo relacionado. En la tercera sección planteamos una adecuación de DTN a la IoT. En la cuarta sección presentamos nuestro trabajo en progreso sobre la seguridad en la IoT. En la quinta sección describimos un escenario de aplicación para la aproximación propuesta. Las conclusiones y las líneas de trabajo futuro cierran el artículo.

II. Seguridad en la IoT

En los trabajos concernientes a la IoT existen dos grandes aproximaciones para convertir el paradigma planteado en una realidad: aproximaciones centralizadas y distribuidas. En las siguientes secciones presentamos la seguridad según los condicionantes de cada una de las visiones y otras propuestas independientes a la aproximación planteada.

II-A. Aspectos de seguridad inherentes al diseño

La IoT [1] es posible gracias a diversas tecnologías que agrupan desde sistemas pasivos de identificación como RFID [5], hasta sistemas más complejos en los que objetos y dispositivos son capaces de generar datos y comunicarse con otros objetos sin necesidad de intervención externa. Las redes de sensores [6] o las redes móviles ad-hoc [7] son otras de las tecnologías que conforman la IoT, juntamente con las redes intracorporales propuestas dentro del ámbito de IoNT [2].

ISBN: 978-84-9717-323-0

La mayoría de aproximaciones ofrecidas para la IoT que se encuentran en funcionamiento acostumbran a tener un diseño centralizado, en el que varios dispositivos identificadores, como podrían ser marcadores RFID o sensores, envían la información a un servidor central, controlado por el proveedor del servicio. La ventaja de estos sistemas es que el fabricante puede ofrecer soluciones de criptografía simétrica entre los dispositivos y el servidor, y posteriormente securizar el servidor con los mecanismos que ofrece una red como Internet en la que existe comunicación de extremo a extremo. Muchas de las propuestas de seguridad concernientes a RFID se basan en este concepto [8], [9].

Otros trabajos, como el presentado en [10], estudian la posibilidad de una IoT distribuida o híbrida en lugar de un esquema completamente centralizado como el mencionado. El esquema distribuido o híbrido supone ciertas desventajas en la aplicación de medidas de seguridad, puesto que se complica la implementación de mecanismos conocidos, como podrían ser sistemas de autenticación basados en una infraestructura de clave pública (PKI, *Private Key Infarestructure*). Por el contrario, el planteamiento de una arquitectura distribuida permite estar más cerca de un paradigma en el que los dispositivos se comunican entre ellos para lograr objetivos comunes o cooperativos en el ámbito local. Un sistema distribuido permite, además, una mayor escalabilidad y, al no estar concentrada toda la inteligencia en un solo dispositivo, posibilita la implementación de políticas de privacidad u otros tratamientos de datos más allá de guardar o recuperar información.

Independientemente del planteamiento distribuido o centralizado, se están realizando esfuerzos para crear estándares necesarios para ofrecer protocolos de comunicación y seguridad adecuados. Uno de los protocolos más usados para conseguir la comunicación entre elementos con restricciones de recursos es ZigBee [11] junto con una adaptación del protocolo IPv6 conocida como LowPan6 [12]. La conjunción de ambos permite trabajar con redes de sensores y redes ad-hoc de manera que cada elemento pueda tener un identificador.

II-B. Soluciones de seguridad

Las propuestas de seguridad especificas para redes ad-hoc móviles, redes inalámbricas malladas [13] o redes de sensores pueden ser buenas aproximaciones para la seguridad en la IoT dado que este tipo de redes se presentan como parte de los bloques que constituyen el paradigma de interconexión de objetos. Por las características de estas redes, los mecanismos criptográficos basados en PKI suponen un sobrecoste que no siempre resulta asumible. Este sobrecoste, añadido al hecho que en las redes de sensores no siempre es posible contactar con una autoridad certificadora, hace que la criptografía basada en PKI no sea siempre una buena solución.

ZigBee aporta, también, sus propios mecanismos de seguridad, aunque están diseñados para redes del tipo muchos a uno. Es decir, no está pensado para una arquitectura distribuida, en la que podría presentar problemas de escalabilidad. Además en [14] se realiza un estudio de varios mecanismos de seguridad para redes inalámbricas malladas (WMN, *Wireless Mesh Networks*) en los que quedan patentes algunos de los problemas de ZigBee respecto a la confidencialidad. Asimismo, el uso de entidades coordinadoras dificultan la gestión de claves.

Algunos estudios, como los presentados en [15], hacen uso de criptografía basada en pairings (PBC *Pairing Based Criptography*) tratando de solventar los problema de gestión de claves que plantean otros sistemas criptográficos. Aún con propuestas que prescinden de usar una PKI, como aquellas basadas en pairings, la distribución de claves en un entorno como el de la IoT, con un gran número de dispositivos conectados, plantea problemas de escalabilidad. Tratando de solventar los problemas de distribución de claves, se encuentran algunas propuestas que ofrecen soluciones mediante criptografía basada en la identidad [16] (IBC, *Identity Based Criptography*).

Los problemas de integridad y confidencialidad, sin embargo, no son los únicos problemas de seguridad que se encuentran en la IoT. Un entorno en el que existen grandes cantidades de objetos interconectados supone un problema para la privacidad y el anonimato de los usuarios. Deben diseñarse sistemas de autenticación que limiten de forma eficiente quien puede recuperar los datos de sensores u otros objetos. En este aspecto, existen estudios como [17] que proponen soluciones a los problemas de autenticación. Otras aproximaciones como la planteada en [18], no hacen uso del citado tipo de criptografía. Sin embargo la propuesta se ha demostrado insegura en [19].

III. Aproximación DTN a la IoT

En esta sección describimos la arquitectura DTN y justificamos la aproximación DTN para la IoT a la vez que revisamos las limitaciones de nuestra aproximación.

III-A. Redes tolerantes a retraos e interrupciones

DTN [4] es una arquitectura de red diseñada para trabajar en entornos sin conectividad extremo a extremo, con grandes retrasos en la comunicación, canales asimétricos y dispositivos heterogéneos. DTN hace uso de mecanismos de *store-carry and forward* que permiten a un nodo almacenar los mensajes mientras no hay comunicación y entregarlos en cuando se produce el contacto con otros nodos. La comunicación de este tipo de redes es, en ocasiones, de tipo oportunista y está supeditada al encuentro con otros nodos. Para garantizar la comunicación extremo a extremo se define el protocolo Bundle [20] que permite la entrega de los mensajes sin importar los protocolos subyacentes. Algunos trabajos presentan enfoques DTN para entornos en los que son aplicables otras arquitecturas, como en [21] para redes de sensores o [22] para redes malladas.

III-B. Aproximación DTN a la IoT

El paradigma IoT se construye a partir de un conjunto de tecnologías heterogéneas que comparten unas restricciones comunes como una capacidad de cómputo limitada y limitaciones energéticas. Sin embargo, no todos los dispositivos en IoT sufren de estas restricciones puesto que existen dispositivos

que poseen mayor capacidad de cálculo y que pueden tener un acceso constante a una fuente de energía.

Dado lo heterogéneo de los dispositivos que pueden conformar IoT, en la aproximación que proponemos se entenderá una región como un conjunto de dispositivos que comparten unas características similares en capacidad de computo, limitaciones de batería y capacidad de interconexión.

Teniendo en cuenta los distintos tipos de dispositivos, la aproximación DTN podría considerar una arquitectura de comunicación híbrida, en la que existen regiones de comunicación muchos a uno, como en el caso de RFID, o muchos a muchos, como el caso de algunas redes de sensores, que además se comunican entre ellas. Así pues, con una arquitectura híbrida los nodos de la DTN equivaldrían a los sensores u objetos capaces de identificarse, como los marcadores RFID. Por otra parte, dispositivos con mayor capacidad de cómputo y batería podrían actuar como mulas de datos, es decir, podrían recoger los datos de otros nodos para reenviarlos. El uso del protocolo Bundle [20] garantizaría las comunicaciones extremo a extremo y su extensión de seguridad permitiría otorgar confidencialidad e integridad a los datos [23]. La finalidad de usar una arquitectura DTN sería proveer comunicación entre las regiones y entre los dispositivos de la misma región. Las características de diseño de la arquitectura DTN complementarían a la IoT supliendo algunas de las restricciones necesarias como falta de disponibilidad, canales asimétricos o el trabajo con dispositivos heterogéneos.

III-C. Limitaciones de nuestra aproximación

En algunos trabajos, como [24], se menciona la posibilidad de una arquitectura DTN para la IoNT. Con la aproximación DTN propuesta, sin embargo, en cada comunicación habría que incorporar la cabecera especificada por el protocolo Bundle a los datos y ello supone una complejidad inasumible En otros escenarios con restricciones en el volumen de datos a transmitir durante la comunicación, las cabeceras del protocolo Bundle supondrían también una limitación considerable.

IV. Seguridad DTN para la IoT

En está sección presentamos los mecanismos de seguridad de DTN y su adaptación a la IoT.

IV-A. Seguridad en DTN

El uso de la extensión de seguridad del protocolo Bundle provee de integridad y confidencialidad a los mensajes enviados de extremo a extremo. Por otra parte, la extensión de seguridad no especifica el tipo de claves criptográficas a usar. IBC ofrece una solución que se adapta a las necesidades de la arquitectura DTN.

IBC propone que la clave pública sea la propia identidad del usuario. Usando la identidad como clave pública, se pretende evitar tener que recurrir a una tercera parte de confianza que provea las claves necesarias. El esquema IBC, sin embargo, es incapaz de eliminarla. Debe existir al menos un generador de claves privadas (PKG, *Private Key Generator*). Resulta necesario que todos los nodos de la red se comuniquen con él para obtener las claves privadas correspondientes a su identidad.

Una aproximación jerárquica de IBC (HIBC, *Hirearchical Identity based cryptography*) [25] ofrece la escalabilidad necesaria tanto en arquitecturas DTN como en el paradigma de la IoT. Algunas implementaciones de HIBC como [26] proponen esquemas en los que el PKG genera las claves privadas para un conjunto de PKGs de nivel inferior, que serán los encargados de generar las claves privadas de un subconjunto de nodos de la red. Con esta propuesta, además de escalabilidad se garantiza que, en caso de quedar comprometido un PKG, no quede comprometido el sistema completo.

Cuando un nodo distinto del PKG queda comprometido es necesario revocar las claves. Sin embargo, dado que HIBC no necesita de una tercera parte para obtener las claves, no es posible comprobar que sigan siendo vigentes. En [27] se soluciona el problema de la revocación de claves mediante la concatenación de una marca de tiempo a la identidad en la generación de las claves públicas. Siendo así, la pareja de claves tiene una duración concreta y, en caso de que estas se vean comprometidas, únicamente lo estarán durante el periodo de tiempo en el que tienen validez.

Existen otras soluciones de seguridad que además de la confidencialidad, cubren problemas como el de la autenticación. En [28] se presenta una aproximación de clave simétrica donde, dado el esquema IBC propuesto por Boneh y Franklin [29], es posible establecer un secreto compartido entre cada pareja de nodos. Lo interesante de la propuesta reside en la posibilidad de generar el secreto compartido de forma no interactiva. De esta manera, en redes donde los contactos son oportunistas o donde existen limitaciones de cómputo, dos usuarios con las parejas de claves

$$(ID_U, d_U), (ID_V, d_V)$$

podrán calcular el secreto compartido entre ambos de forma independiente como:

$$K_{UV} = e(Q_U, d_V) = e(Q_V, d_U) = e(Q_U, Q_V)^s$$

donde s es el secreto maestro que únicamente conoce el PKG y $Q_U = H(ID_U)$ i $Q_V = H(ID_V)$ siendo H una función resumen. La igualdad expuesta, implica que el PKG tiene acceso al contenido de las comunicaciones, aún cuando dos nodos se hayan autenticado mutuamente y establecido un canal seguro.

IV-B. Adaptación a la IoT

Dado el requisito de escalabilidad que se debe cumplir en la IoT, proponemos como solución un sistema jerárquico de IBC como el propuesto en [26] que permite la creación de regiones, con un PKG por región y un nodo central que genera las claves para los PKG de cada una de las regiones. Junto con el sistema HIBC consideramos una marca temporal para gestionar la revocación de claves. Aunque el uso de marcas de tiempo da robustez y soluciona el problema de la revocación, supone que los nodos de la red deberán almacenar N claves. Sin embargo, en algunas ocasiones los nodos de la IoT tendrán

restricciones de memoria y ello podría generarles una excesiva dependencia con el PKG.

Tratando de solventar la dependencia que podría llegar a generarse con el PKG, y tratando de evitar también la capacidad de computo que se puede requerir para generar el canal seguro mediante el cifrado de cada mensaje con claves IBC, proponemos un esquema de clave simétrica basado en HIBC. La generación de claves simétricas para la autenticación mutua permite la creación de un canal seguro y auténtico sin la necesidad de usar las claves asimétricas. El uso exclusivamente privado de las claves IBC permitiría alargar su vida útil y reducir la dependencia del nodo con el PKG. Además, una vez calculada la clave, las operaciones para cifrar y descifrar no supondrán el mismo coste computacional que supondrían las operaciones en curvas elípticas en las que se basa IBC. Conseguimos entonces una reducción de la energía consumida por los nodos. Si tenemos en cuenta la propuesta [28], sería posible la generación de la clave simétrica de manera no interactiva, permitiendo un canal seguro y auténtico sin intercambio previo a la comunicación de datos.

Con la propuesta de la clave simétrica pretendemos también dotar de cierta protección contra la impersonalización en la solicitud de claves al PKG. Si consideramos que en la IoT los nodos que se agregan a una región no tienen que provenir de fuentes de confianza, estos podrían tomar la identidad de otro nodo frente al PKG y solicitar claves privadas. Con dicha solicitud conseguirían las claves privadas de otro nodo, pudiendo acceder a sus mensajes o actuar de forma deshonesta en su nombre.

Si asumimos que el PKG es habitualmente un nodo con más recursos de cómputo y memoria que el resto de los nodos se puede considerar la siguiente aproximación:

- Cuando un nodo (N) solicita claves por primera vez ante el PKG este comprueba si ya ha provisto de claves al nodo solicitante. Si es la primera solicitud, almacena la identidad del nodo y genera las claves correspondientes.
- Al solicitar claves de nuevo, el nodo envía al PKG la tupla (ID_N, $E_{K_{NPKG}}(ID_N)$).
- El PKG extrae el timestamp de ID_N y calcula el secreto compartido K_{NPKG}, entonces si $D_{K_{NPKG}}(ID_N) = ID_N$ genera la claves y las remite al nodo.

donde $E_{K_{NPKG}}(ID_N)$ es la identidad del nodo cifrada haciendo uso del secreto compartido entre el PKG y el nodo y K_{NPKG} es el secreto compartido. Es necesario recordar que el PKG no precisa de clave privada para realizar el cálculo del secreto compartido (véase IV-A). La extracción de la marca de tiempo de la identidad provista se plantea necesario debido a que en el momento de solicitar nuevas claves es posible que aquellas que almacena el nodo ya no tengan validez. La generación de la clave simétrica por parte del PKG, sin embargo, no requiere de la clave privada correspondiente a una determinada identidad. Gracias a esta característica es posible para el PKG validar la clave simétrica aún cuando la clave pública correspondiente haya caducado.

V. Escenario de aplicación

En esta sección se plantea un escenario de aplicación típico de la IoT y la aproximación DTN que le correspondería. Se pretende mostrar la adaptación de la aproximación propuesta para la IoT en un escenario real.

Un escenario típico en el campo de la IoT es la monitorización de la salud del usuario mediante pulseras o prendas de ropa con los sensores adecuados. Con la monitorización de la salud en mente, se plantea un escenario en el que diversos grupos de bomberos intentan apagar un incendio forestal. Los bomberos van equipados con trajes capaces de monitorizar sus constantes vitales y sus signos de fatiga. En el bosque no hay posibilidad de conseguir una conexión a Internet para mandar los datos al centro de mando.

Los vehículos que ayudan en las tareas de extinción cuentan con dispositivos que soportan la comunicación mediante el protocolo Bundle y que pueden entrar en comunicación con las unidades terrestres cuando estas se encuentran dentro del radio de acción del dispositivo. Los vehículos captan los datos de las unidades terrestres y al ir a recargar las cubas transmiten la información al centro de mando. Entonces los datos son procesadas y se pueden mandar ordenes de vuelta.

En este escenario los objetos, los trajes de los bomberos, son capaces de comunicarse con la central mediante el uso del protocolo Bundle y transmitir los datos adecuados para la correcta gestión de las unidades durante el incendio. Además, los trajes son capaces de recibir ordenes y transmitirlas a sus usuarios según lo considere el centro de coordinación.

El uso del protocolo Bundle junto con un sistema de seguridad resulta imprescindible. El protocolo Bundle asegura que se pueda producir la comunicación extremo a extremo, incluso cuando las conexiones con los vehículos son esporádicas. La seguridad garantiza que ninguna persona no autorizada pueda tener acceso a los datos de los bomberos o a las ordenes de la central. Para ello, los trajes de los bomberos pueden contar con claves simétricas creadas a partir de su número de identificación dentro del cuerpo de bomberos y de la identificación del vehículo, a partir de la matricula por ejemplo. El uso de las claves simétricas pre-computadas permitiría el intercambio rápido de mensajes en el tiempo limitado en que un camión o hidroavión se encontrase cerca de una unidad de extinción. Si los vehículos actúan, además, como nodos de confianza se pueden renovar las claves periódicamente gracias a una organización HIBC.

La aproximación DTN al escenario de la IoT permite la monitorización de los cuerpos de extinción, aún cuando estos se encuentren dispersos y fuera del alcance de comunicación con los vehículos. De esta manera es posible una gestión completa del operativo de forma segura.

VI. Conclusiones y trabajo futuro

En este trabajo hemos presentado una visión de la IoT y alguna de las medidas de seguridad que se han estudiado para el paradigma de la IoT. Hemos presentado, además, una aproximación DTN para la comunicación en la IoT y hemos revisado alguno de los mecanismos de seguridad que existen

para la arquitectura DTN, y que pueden ser adaptados a la IoT. Hemos considerado también alguna de las limitaciones existentes para la aproximación propuesta.

Como trabajo futuro deberíamos adaptar la propuesta de uso de las claves simétricas a la aproximación jerárquica de IBC para poder permitir el establecimiento de un canal seguro entre nodos pertenecientes a distintas regiones. Además, el cambio de región de un nodo no debería suponer un problema para obtener claves de un nuevo PKG. La posibilidad de realizar la solicitud de claves a otro PKG está estrechamente relacionada con la adaptación del mecanismo de identificación mutua en HIBC.

Sería también una línea de trabajo interesante estudiar la posibilidad de adaptar el protocolo Bundle para situaciones en que el sobrecoste de enviar las cabeceras hace inviable el uso de una aproximación DTN, por ejemplo en el caso de nano-dispositivos.

AGRADECIMIENTOS

Este trabajo ha sido parcialmente financiado por el Ministerio de Ciencia e Innovación Español, proyecto TIN2010-15764 y por la Generalitat de Cataluña, proyecto 2014SGR-619.

REFERENCIAS

[1] R. H. Weber and R. Weber, *Internet of Things*. Springer, 2010.
[2] I. F. Akyildiz and J. M. Jornet, "The internet of nano-things," *Wireless Communications, IEEE*, vol. 17, no. 6, pp. 58–63, 2010.
[3] M. A. Feki, F. Kawsar, M. Boussard, and L. Trappeniers, "The internet of things: The next technological revolution," *Computer*, vol. 46, no. 2, pp. 24–25, 2013.
[4] K. Fall, "A delay-tolerant network architecture for challenged internets," in *Proceedings of the 2003 conference on Applications, technologies, architectures, and protocols for computer communications*, pp. 27–34, ACM, 2003.
[5] K. Finkenzeller, *RFID Handbook*. Wiley Online Library, 2003.
[6] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless sensor networks: a survey," *Computer networks*, vol. 38, no. 4, pp. 393–422, 2002.
[7] S. Basagni, M. Conti, S. Giordano, and I. Stojmenovic, *Mobile ad hoc networking*. John Wiley & Sons, 2004.
[8] G. Hancke, K. Markantonakis, and K. Mayes, "Security challenges for user-oriented RFID applications within the Internet of Things," *Journal of Internet Technology*, vol. 11, no. 3, pp. 307–313, 2010.
[9] A. Juels, "RFID security and privacy: A research survey," *Selected Areas in Communications, IEEE Journal on*, vol. 24, no. 2, pp. 381–394, 2006.
[10] R. Roman, J. Zhou, and J. Lopez, "On the features and challenges of security and privacy in distributed Internet of Things," *Computer Networks*, vol. 57, no. 10, pp. 2266–2279, 2013.
[11] ZigBee Alliance, "Zigbee specification," *URL: http://www. zigbee. org*, vol. 558, 2006.
[12] G. Mulligan, "The 6LoWPAN architecture," in *Proceedings of the 4th workshop on Embedded networked sensors*, pp. 78–82, ACM, 2007.
[13] I. F. Akyildiz, X. Wang, and W. Wang, "Wireless mesh networks: a survey," *Computer networks*, vol. 47, no. 4, pp. 445–487, 2005.
[14] C. Alcaraz and J. Lopez, "A security analysis for wireless sensor mesh networks in highly critical systems," *Systems, Man, and Cybernetics, Part C: Applications and Reviews, IEEE Transactions on*, vol. 40, no. 4, pp. 419–428, 2010.
[15] P. Szczechowiak, A. Kargl, M. Scott, and M. Collier, "On the application of pairing based cryptography to wireless sensor networks," in *Proceedings of the second ACM conference on Wireless network security*, pp. 1–12, ACM, 2009.
[16] A. Shamir, "Identity-based cryptosystems and signature schemes," in *Advances in cryptology*, pp. 47–53, Springer, 1985.
[17] G. Zhao, X. Si, J. Wang, X. Long, and T. Hu, "A novel mutual authentication scheme for internet of things," in *Modelling, Identification and Control (ICMIC), Proceedings of 2011 International Conference on*, pp. 563–566, IEEE, 2011.
[18] A. Alcaide, E. Palomar, J. Montero-Castillo, and A. Ribagorda, "Anonymous authentication for privacy-preserving IoT target-driven applications," *Computers & Security*, vol. 37, pp. 111–123, 2013.
[19] X. J. Lin and L. Sun, "Insecurity of an anonymous authentication for privacy-preserving IoT target-driven applications," *IACR Cryptology ePrint Archive*, vol. 2013, p. 795, 2013.
[20] K. L. Scott and S. Burleigh, "Bundle protocol specification," 2007.
[21] C. Borrego and S. Robles, "A store-carry-process-and-forward paradigm for intelligent sensor grids," *Information Sciences*, vol. 222, no. 0, pp. 113 – 125, 2013.
[22] C. Borrego, S. Castillo, and S. Robles, "Striving for sensing: Taming your mobile code to share a robot sensor network," *Information Sciences*, 2014.
[23] S. Symington, S. Farrell, H. Weiss, and P. Lovell, "Bundle security protocol specification," *Work Progress, October*, 2007.
[24] S. Balasubramaniam and J. Kangasharju, "Realizing the internet of nano things: challenges, solutions, and applications," *Computer*, vol. 46, no. 2, pp. 62–68, 2013.
[25] C. Gentry and A. Silverberg, "Hierarchical ID-based cryptography," in *Advances in cryptology-ASIACRYPT 2002*, pp. 548–566, Springer, 2002.
[26] R. Patra, S. Surana, and S. Nedevschi, "Hierarchical identity based cryptography for end-to-end security in DTNs," in *Intelligent Computer Communication and Processing, 2008. ICCP 2008. 4th International Conference on*, pp. 223–230, IEEE, 2008.
[27] A. Seth and S. Keshav, "Practical security for disconnected nodes," in *Secure Network Protocols, 2005.(NPSec). 1st IEEE ICNP Workshop on*, pp. 31–36, IEEE, 2005.
[28] R. Dupont and A. Enge, "Provably secure non-interactive key distribution based on pairings," *Discrete Applied Mathematics*, vol. 154, no. 2, pp. 270–276, 2006.
[29] D. Boneh and M. Franklin, "Identity-based encryption from the Weil pairing," in *Advances in Cryptology-CRYPTO 2001*, pp. 213–229, Springer, 2001.