R. Rios, and J. Lopez, "Evolución y nuevos desafios de privacidad en la Internet de las Cosas", *XIV Reunión Española sobre Criptología y Seguridad de la Información*, pp. 209-213, 2016.
NICS Lab. Publications: https://www.nics.uma.es/publications

Evolución y nuevos desafios de privacidad en la Internet de las Cosas

Ruben Rios
Lenguajes y Ciencias de la Computación
Universidad de Málaga
Email: ruben@lcc.uma.es

Javier Lopez
Lenguajes y Ciencias de la Computación
Universidad de Málaga
Email: jlm@lcc.uma.es

Resumen

La Internet de las Cosas (en inglés, *Internet of Things* (IoT)) es una evolución de la Internet tal y como lo conocemos. Esta versión aumentada de Internet incorpora objetos de la vida cotidiana, rompiendo así barrera de los digital y extendiéndose al mundo físico. Estos objetos interactuarán entre sí y con otras entidades tanto de manera local como remota, y estarán dotados de cierta capacidad computacional y sensores para que sean conscientes de lo que ocurre en su entorno. Esto traerá consigo un sinfín de posibilidades y nuevos servicios, pero también dará lugar a nuevos y mayores riesgos de privacidad para los ciudadanos. En este artículo, estudiamos los problemas de privacidad actuales de una de las tecnologías claves para el desarrollo de este prometedor paradigma, las redes de sensores, y analizamos como pueden evolucionar y surgir nuevos riesgos de privacidad al ser completamente integradas en Internet.

Desafíos (*Challenges*), Internet de las Cosas (*Internet of Things*), Privacidad (*Privacy*), Sensores (*Sensors*)

1. Introducción

Internet está cambiado y pronto dejará de ser una red ordenadores y pasará a integrar elementos físicos del mundo real, ya sean coches, juguetes o personas. De hecho, la composición de Internet y el uso que hacemos de ella hace tiempo que ha cambiado. Gigantes como Google afirman que reciben más consultas desde teléfonos móviles que desde equipos de sobremesa y portátiles [1]. Aunque esto supone un cambio, éste se refiere únicamente al interfaz de comunicación con Internet y no a la estructura de Internet en sí misma. No obstante, con la Internet de las Cosas (IoT) [2], no sólo cambia el interfaz sino que además cambia su propia arquitectura. Los objetos de la vida real, no sólo teléfonos móviles sino también otros objetos, dejan de ser meros consumidores de datos

y pasan a ofrecer datos y servicios aumentados con la información que obtienen de su entorno.

La realización de este nuevo paradigma traerá consigo numerosos beneficios tanto para la industria como para las personas. Sin embargo, el despliegue de tecnologías capaces de monitorizar y compartir información detallada sobre su entorno, como aquellas encontradas bajo el paraguas de la Internet de las Cosas, abre la puerta a numerosos problemas de privacidad. Hasta la fecha, los usuarios de internet ponían en riesgo su privacidad cuando eran una parte activa de Internet, es decir, cuando solicitaban servicios determinados. En el futuro, los individuos se encontrarán constantemente expuestos a tecnologías capaces de recolectar información sobre ellos sin ni siquiera ser conscientes, en muchos casos, de ser el objeto de tal recolección de datos. Por ejemplo, habrá sensores en nuestras casas monitorizando el consumo eléctrico, en nuestros coches controlando la velocidad y rutas que conducimos, e incluso en nuestra ropa y acoplados a nuestro cuerpo vigilando nuestras constantes vitales.

Con todo esto es razonable que haya detractores de la IoT en diferentes sectores de la sociedad que alegan que la llegada de este nuevo paradigma traerá consigo una serie de riesgos de privacidad sin precedentes, haciendo del mundo un lugar con mayor control y menos libertades para los ciudadanos [3]. Para evitar este tipo de reticencias y promover la aceptación de la IoT es necesario analizar y prever posibles amenazas de privacidad en estos entornos. Sólo así será posible establecer las medidas oportunas para afrontar posibles problemas y dar rienda suelta al IoT y a todos sus beneficios. Por ello, el objetivo principal de este trabajo es analizar escenarios en los que intervienen redes de sensores y evaluar si los problemas de privacidad existentes en estos escenarios serán heredados por la IoT. Además, se identifican nuevos desafíos y amenazas de privacidad que surgen de la integración de los sensores en Internet.

A continuación, en la sección 2, se ofrece una breve revisión de los elementos comunes y diferencias más significativas entre las redes de sensores y la Internet de las Cosas. Asimismo, esta sección ofrece un clasificación de los problemas de privacidad presentes en redes de sensores. Seguidamente, las secciones 3 y 4 se centran en dos de estos grandes grupos de problemas, señalando las soluciones actuales y desafíos futuros. Tras esto, la sección 5 identifica nuevos desafíos de privacidad inherentes a la IoT y, finalmente, la sección 6 ofrece un breve resumen y conclusiones del trabajo.

2. Preliminares

En sus comienzos, se pretendía implementar la IoT acoplando etiquetas RFID a los objetos de nuestro entorno [4]. Sin embargo, con el paso del tiempo, esta visión original se ha ido extendido para integrar nuevas tecnologías y aumentar así sus capacidades. Entre las tecnologías más importantes de esta nueva visión, se encuentran las tecnologías de sensores, que le confieren a la IoT la posibilidad de sentir y razonar acerca del mundo físico.

2.1. Escenario

Las redes de sensores (en inglés, *Wireless Sensor Networks* (WSNs)) [5] son sistemas altamente distribuidos compuestos por dispositivos de capacidades li-

mitadas y dotados de interfaces de comunicación inalámbrica y sensores físicos. Estas redes suelen seguir un modelo de comunicación multi-salto para hacer llegar los datos recogidos por los nodos sensores hasta un dispositivo de recolección y análisis, llamado estación base. En cierto modo, la IoT tiene una estructura muy similar a las WSNs con una capa de objetos inteligentes que recogen información sobre su entorno y finalmente se envían a servidores en la nube para procesar los datos (figura 1).

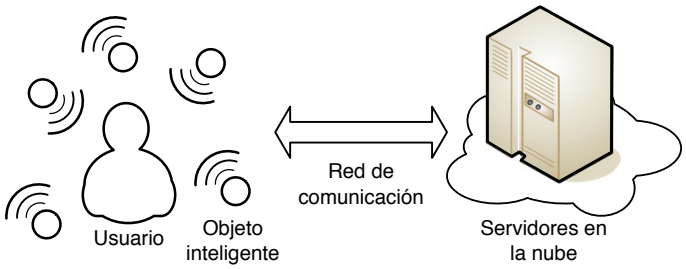

Figura 1: Visión general de la IoT

La mayor diferencia entre ambos modelos radica en la forma en que los elementos de la capa de recolección se comunican. Los objetos de la IoT suelen estar conectados directamente a Internet, así que por lo general no recurren a otros objetos para enviar sus datos a los servidores en la nube. Además, los datos recolectados suelen ser utilizados para ofrecer servicios avanzados a los usuarios, que normalmente los reciben a través de los propios objetos inteligentes. En cambio, lo normal en redes de sensores suele ser que los datos fluyan de los sensores a la estación base, aunque existen modelos de recolección de datos *query-driven*, en los que la estación base realiza las consultas a la red y los sensores responden a estas consultas.

2.2. Privacidad en WSN

Los problemas de privacidad en redes de sensores pueden clasificarse en dos grandes grupos [6] en función de la entidad que se ve amenazada:

- Los problemas *user-centric* afectan a los individuos que, al encontrarse en las inmediaciones de la red, pueden ser monitorizados sin su consentimiento. Las redes de sensores se convierten, por tanto, en una tecnología capaz de invadir la privacidad de los usuarios.
- Los problemas *network-centric* afectan a la propia red y a los elementos monitorizados por ella. En este caso, el atacante es una entidad externa que se aprovecha del despliegue de la red para obtener información sensible.

En este trabajo nos centraremos en los problemas *network-centric* ya que los problemas *user-centric* no son fácilmente abordables desde un punto de vista tecnológico y suelen ser abordados desde una perspectiva legislativa, a través regulaciones y directivas [7]. Por su parte, los problemas *network-centric* pueden a su vez dividirse en varias categorías dependiendo del tipo de información o recurso que se quiere proteger (figura 2). En las siguientes secciones analizaremos

cada uno de estos problemas y discutiremos de qué forma se ven estos afectados por la integración de las redes de sensores en Internet.

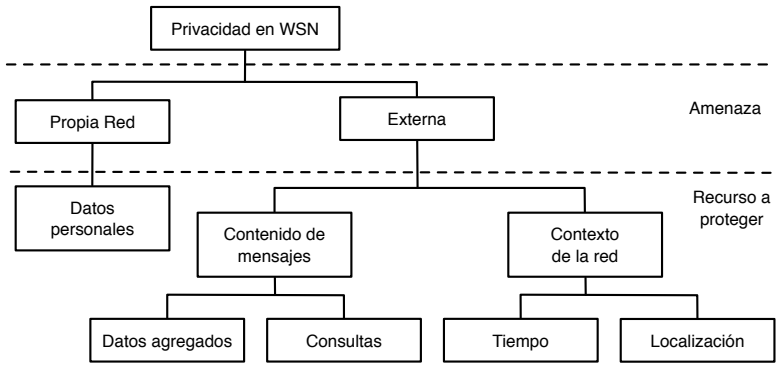

Figura 2: Clasificación de problemas

3. Protección del Contenido

El punto de partida para proporcionar privacidad es proteger el contenido de los mensajes. Aunque el enfoque tradicional para proteger los datos se basa en el uso de mecanismos de autenticación y cifrado, estos mecanismos no son suficientes durante el proceso de agregación de datos ni tampoco cuando se envían consultas a los nodos de la red.

3.1. Datos agregados

La agregación de datos es un proceso que ayuda a los nodos a ahorrar recursos y energía. Cuando un nodo recibe un paquete que debe ser reenviado a la estación base, éste puede aprovechar para incluir sus propios datos en el mensaje. Dado que el nodo debe ser capaz de manipular el contenido del mensaje para realizar esta tarea, el mensaje no puede estar cifrado extremo a extremo y, por ende, existe un riesgo de privacidad sobre los datos si el nodo es malicioso.

En la literatura existen diversos enfoques para hacer frente a este problema. Uno de los enfoques principales se basa en la utilización de cifrado homomórfico [8] para poder aplicar ciertas operaciones sobre los mensajes sin revelar su contenido. Sin embargo, el coste computacional de este tipo de cifrado suele ser excesivo para las capacidades de dispositivos sensores. Por ello, otros autores se han centrado en la fragmentación de datos [9] y en la perturbación de los datos mediante generalización [10] o la adición de ruido [11].

Existen varios *desafíos* relacionados con la agregación de datos en la IoT. En primer lugar, la mayoría de soluciones anteriores asumen topologías de redes particulares, organizadas en clústers y donde los nodos son estáticos. No obstante, los escenarios previstos en la IoT serán altamente cambiantes. Relacionado con esto, existe un claro problema de distribución de claves y confianza. Esto apunta a la necesidad de utilizar mecanismos de clave publica, pero la cantidad y heterogeneidad de los dispositivos así como la limitación de recursos suponen barreras importantes en este sentido. Asimismo, es importante avanzar en el

desarrollo de mecanismos completamente homomórficos capaces de ser ejecutados en dispositivos altamente restringidos. Por último, también es necesario considerar la presencia de atacantes activos que, además de observar el contenido de los mensajes, modifican los valores para que el resultado agregado sea incorrecto y, en tal caso, revelar su identidad.

3.2. Consultas

Las redes de sensores suelen seguir un método de comunicación basado en eventos. Sin embargo, hay redes que optan por modelos basados en consultas y permiten a los usuarios solicitar información sobre determinados sensores. Esto, que aparentemente no entraña mayor riesgo, supone un importante problema de privacidad ya que un atacante observando las comunicaciones puede aprender los intereses del usuario (e.g., zona con posibles reservas de petróleo) en función de los nodos que respondan a la consulta.

La solución más sencilla y eficaz a este problema es que todos los nodos respondan ante cualquier consulta y sea el usuario el que descarte los datos que no le sean relevantes. Esta solución es también la más costosa. A fin de reducir el coste, algunos autores han optado por combinar esta solución con técnicas de agregación de datos [12]. También se ha propuesto el envío consultas falsas [13] para ocultar los intereses reales y por almacenar réplicas de los datos de los sensores en diferentes nodos de la red [14], desvinculando así el nodo que responde de su origen.

Uno de los *desafíos* más importantes en la IoT, se debe a la aparición de nuevos dominios de confianza. En escenarios IoT, la entidad que realiza la consulta no es necesariamente la misma que administra la red. Se trata, por tanto, de un problema similar al de recuperación de información privada de una base de datos [15]. Asimismo, es necesario considerar que los usuarios podrán solicitar datos no sólo de una única red sino de cualquier red disponible a través de Internet, lo que puede revelar intereses de los usuarios en función de las redes con las que se comunican. También es necesario ocultar el patrón de acceso, es decir, la asiduidad y número de consultas, así como el orden en el que se hacen, ya que esto puede revelar el nivel de interés en los datos o el objetivo de las consultas.

4. Protección del Contexto

El contenido de los paquetes no es la única información sensible a proteger durante una comunicación, también el contexto asociado a esa comunicación es importante. El contexto es todo aquello asociado al funcionamiento de la red, incluyendo los eventos que se detectan, el momento en el que se envían mensajes o los nodos que los envían. Esta información puede obtenerse mediante técnicas de análisis de tráfico independientemente de si la confidencialidad de los paquetes intercambiados se encuentra debidamente protegida mediante mecanismos criptográficos.

4.1. Tiempo

La ocurrencia de un evento está siempre asociada al tiempo en el que este evento fue detectado y sin esta información el evento resulta de poco o ningún interés. Por ello, los nodos suelen enviar paquetes inmediatamente después de detectar eventos en su entorno. Precisamente por ello, un atacante puede estimar con cierta precisión el tiempo en el que tiene lugar un evento con datos que pueden obtenerse mediante la mera observación de las comunicaciones: el tiempo de llegada y la distancia al origen. Esto permite al atacante predecir, en ciertos casos, el comportamiento futuro de determinados fenómenos que se repiten en el tiempo.

Ante este problema, la solución más sencilla es que los nodos transmitan a intervalos regulares, pero esto da lugar a retrasos innecesarios en los envíos si estos se encuentran muy espaciados en el tiempo o a un mayor consumo energético si los intervalos son cortos. Existen pocas soluciones que hayan prestado atención a este problema. En [16] se propone que los nodos vayan introduciendo retrasos aleatorios antes de reenviar sus mensajes. El problema es que estos retrasos deben ser suficientemente largos o el atacante seguirá siendo capaz de obtener una buena precisión. Recientemente se ha propuesto una solución similar basada en la adición de retrasos que siguen una distribución laplaciana [17] para perturbar el orden y tiempo de llegada. No obstante, no queda claro que esto suponga un verdadero avance para evitar el problema comentado anteriormente.

Este problema seguirá suponiendo un *desafío* en entornos IoT ya que parece complicado encontrar un equilibrio adecuado entre privacidad temporal y las necesidades de tiempo real de estas redes. Además, la introducción de retrasos en el envío puede entrar en conflicto con otros sistemas de seguridad (i.e., sistemas de detección de intrusiones) presentes en la red. Más allá de la introducción de retrasos, el uso de paquetes falsos o de técnicas esteganográficas para ocultar la existencia de eventos puede ser de gran utilidad. De hecho, este tipo de técnicas ya se han utilizado con éxito para ocultar otro tipo de información de contexto, como veremos a continuación.

4.2. Localización

Los protocolos de comunicación utilizados en WSNs exponen la posición de nodos importantes en la red. Por un lado, revelan la localización de los nodos que generan mensajes y que, por tanto, están próximos a un evento de interés (e.g., la presencia de un carro de combate en un campo de batalla). Por otro lado, también exponen la posición de la estación base, que es el nodo más importante de la red ya que es el encargado de procesar todos los mensajes y, por tanto, debe recibir una protección física especial.

En la literatura se distinguen dos tipos generales de atacantes: los atacantes *locales*, que tienen un rango de actuación reducido y se mueven en las inmediaciones de la red siguiendo el tráfico generado por los nodos; y los atacantes *globales* que pueden monitorizar todas las comunicaciones en remoto, sin necesidad de desplazarse por el terreno. La mayoría de soluciones para hacer frente a atacantes locales se basan en la aleatorización de los caminos seguidos por los paquetes [18, 19], aunque también se ha recurrido a técnicas más avanzadas como, por ejemplo, la ocultación de datos en mensajes de configuración [20]. En cambio, para hacer frente a atacantes globales suele recurrirse a la introducción

de tráfico falso y así ocultar los patrones de envío [21] u homogeneizar el tráfico en la red [22]. Por último, también se ha considerado el problema de atacantes activos, capaces de comprometer nodos con el fin de determinar el origen de eventos [23] o la posición de la estación base [24].

La dimensión de la IoT dará lugar a nuevos escenarios y *desafios* relacionados con la localización. En primer lugar, los modelos de atacantes serán locales a una o varias redes, mientras que el modelo global será prácticamente irrealizable porque para ello sería necesaria controlar todos los flujos de información dentro de la IoT. Dado que habrá más dispositivos, el atacante tendrá más facilidad para comprometer nodos y será necesario prestar mayor atención a este tipo de atacante. Además, es necesario tener en cuenta de que atacante podrá tomar control de ellos y monitorizar las comunicaciones en remoto, a través de Internet. Por otra parte, con la IoT se abren nuevas opciones para evitar la captura de tráfico por parte de atacantes locales ya que los dispositivos podrán optar por comunicar sus datos directamente a través de Internet en lugar de utilizar comunicaciones multi-salto. En lo que respecta a atacantes con mayor rango de acción, habrá que repensar las soluciones basadas en la inyección de tráfico falso dado que habrá muchos más dispositivos y, por consiguiente, más interferencias en el canal. Un área de investigación prometedora para evitar estos problemas es el de las redes cognitivas. Por último, es necesario avanzar en el desarrollo de soluciones frente a atacantes activos, por ejemplo basados en la creación de interferencias para congestionar ciertos caminos de comunicación. Este tipo de ataques no ha sido tenido en cuenta hasta la fecha.

5. Nuevos Desafíos

Además de los problemas heredados de las redes de sensores, la IoT introduce nuevos desafíos debido a la naturaleza dinámica y cambiante del paradigma. En primer lugar, es necesario considerar la IoT como un todo donde los diferentes proveedores de servicio tendrán que compartir los datos que recolectan sus redes de sensores para alcanzar todo su potencial. Así pues, será necesario avanzar en el desarrollo de mecanismos de minado de datos capaces de operar con datos cifrados y/o repartidos en diferentes dominios de confianza.

Con la llegada de la IoT, el usuario deja de ser un elemento pasivo del sistema y comienza a tener responsabilidades sobre determinados objetos. Tendrá que configurar sus propias políticas de compartición de datos y esto no sólo afectará a su privacidad sino también a la de sus familiares y conocidos. Por tanto, será fundamental sensibilizar a la sociedad al respecto de los problemas de privacidad existentes debido a configuraciones vagas. Además, los usuarios deberán tener en cuenta que al prestar sus dispositivos personales o venderlos pueden estar poniendo en riesgo su privacidad. Será necesario, por tanto, establecer mecanismos de borrado u ofuscación de datos para evitar la exfiltración de información en estos casos.

Un área de especial relevancia para la privacidad está relacionada con la forma en la que los usuarios interactúan con los dispositivos. Por un lado, está el problema de presentar a los usuarios información como políticas de privacidad o informes de consentimiento sin los interfaces adecuados. Por otro lado, está el problema de que los interfaces de comunicación con los dispositivos son cada vez más invasivos. Algunos de estos permiten interactuar con los nuestros

dispositivos mediante comandos de voz pero ya existen empresas que están desarrollando tecnologías basadas en el reconocimiento de las ondas cerebrales [25]. Esto tendrá un claro impacto sobre la privacidad ya que no sólo las cosas que hacemos o decimos serán vigiladas sino que también estará en el punto de mira aquello que pensamos.

Por último, a medida que avance el desarrollo de la IoT, los objetos que la conforman interactuarán con otros objetos o personas y no sólo con una estación base o pasarela. Las interacciones de entre objetos puede dar lugar a la creación de grafos de relación aumentados, como los presentes en redes sociales. Esto permitiría a un atacante determinar no sólo los objetos que poseemos sino también con qué otros objetos o personas interactúan, revelando así nuestros intereses y actividades profesionales e incluso nuestras relaciones personales, entre otras muchas cosas.

6. Conclusión

En este trabajo se ha discutido sobre una serie de problemas de privacidad que pueden dificultar el desarrollo y aceptación de la Internet de las Cosas debido al uso de tecnologías invasivas, como las redes de sensores. Estos problemas viene derivados, por una parte, de su capacidad para recolectar y compartir información detallada sobre su entorno y, por otra parte, de su propias limitaciones hardware y modo de funcionamiento. Se han presentado diferentes categorías de problemas y analizado las actuales medidas de protección. Asimismo, se ha tratado de prever cómo evolucionaran estos problemas al integrar las tecnologías de sensores en Internet. Finalmente, se han identificado una serie de problemas que no están directamente relacionados con problemas ya existentes sino que viene derivados directamente de las características propias de la IoT, pero que sin duda afectarán a nuestra privacidad en el futuro.

Agradecimientos

Este trabajo ha sido posible gracias a la financiación del Ministerio de Economía y Competitividad y de la Junta de Andalucía a través de los proyectos PERSIST (TIN2013-41739-R) y FISICCO (P11-TIC-07223), respectivamente.También ha sido financiado parcialmente por la Red de Formación NeCS del Programa Marie Curie del Programa H2020 (H2020-MSCA-ITN-2015-675320).

Referencias

[1] G. Sterlin, "It's Official: Google Says More Searches Now On Mobile Than On Desktop," May 2015, [Online]. Available: http://searchengineland.com/its-official-google-says-more-searches-now-on-mobile-than-on-desktop-220369.

[2] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions," *Future Generation Computer Systems*, vol. 29, no. 7, pp. 1645 – 1660, 2013.

[3] P. N. Howard, *Pax Technica: How the Internet of Things May Set Us Free or Lock Us Up.* Yale University Press, 2015, ISBN 978-0-300-19947-5.

[4] CERP-IoT, "Visions and Challenges for Realising the Internet of Things," European Commision, Tech. Rep., March 2010. [Online]. Available: http://www.internet-of-things-research.eu/pdf/IoT_Clusterbook_March_2010.pdf

[5] P. Rawat, K. Singh, H. Chaouchi, and J. Bonnin, "Wireless sensor networks: a survey on recent developments and potential synergies," *The Journal of Supercomputing*, vol. 68, no. 1, pp. 1–48, 2014.

[6] R. Rios and J. Lopez, "Analysis of Location Privacy Solutions in Wireless Sensor Networks," *IET Communications*, vol. 5, pp. 2518 – 2532, 2011.

[7] Parlamento Europeo y Consejo de la Unión, "Directiva 95/46/CE relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos," Nov 1995. [Online]. Available: http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:31995L0046&from=ES

[8] S. Othman, A. Bahattab, A. Trad, and H. Youssef, "Confidentiality and Integrity for Data Aggregation in WSN Using Homomorphic Encryption," *Wireless Personal Communications*, vol. 80, no. 2, pp. 867–889, 2015.

[9] G. Yang, S. Li, X. Xu, H. Dai, , and Z. Yang, "Precision-Enhanced and Encryption-Mixed Privacy-Preserving Data Aggregation in Wireless Sensor Networks," *International Journal of Distributed Sensor Networks*, vol. 2013, no. 427275, p. 12, 2013.

[10] W. Zhang, C. Wang, and T. Feng, "GP2S: Generic Privacy-Preservation Solutions for Approximate Aggregation of Sensor Data," in *Sixth Annual IEEE International Conference on Pervasive Computing and Communications (PerCom 2008).* Hong Kong, China: IEEE Computer Society, Washington, DC, USA, 17-21 March 2008, pp. 179 –184.

[11] S. Ozdemir, M. Peng, and Y. Xiao, "PRDA: polynomial regression-based privacy-preserving data aggregation for wireless sensor networks," *Wireless Communications and Mobile Computing*, vol. 15, no. 4, pp. 615–628, 2015.

[12] R. Di Pietro and A. Viejo, "Location privacy and resilience in wireless sensor networks querying," *Comput. Commun.*, vol. 34, no. 3, pp. 515–523, March 2011.

[13] B. Carbunar, Y. Yu, W. Shi, M. Pearce, and V. Vasudevan, "Query privacy in wireless sensor networks," *ACM Trans. Sen. Netw.*, vol. 6, no. 2, pp. 14:1–14:34, Mar. 2010.

[14] T. Dimitriou and A. Sabouri, "Privacy preservation schemes for querying wireless sensor networks," in *IEEE International Conference on Pervasive Computing and Communications Workshops,*, 2011, pp. 178–183.

[15] S. Yekhanin, "Private Information Retrieval," *Commun. ACM*, vol. 53, no. 4, pp. 68–73, Apr. 2010.

[16] P. Kamat, W. Xu, W. Trappe, and Y. Zhang, "Temporal Privacy in Wireless Sensor Networks: Theory and Practice," *ACM Trans. Sen. Netw.*, vol. 5, no. 4, pp. 28:1–28:24, Nov. 2009.

[17] X. Yang, X. Ren, S. Yang, and J. McCann, "A novel temporal perturbation based privacy-preserving scheme for real-time monitoring systems," *Computer Networks*, vol. 88, pp. 72 – 88, 2015.

[18] R. Rios and J. Lopez, "Exploiting Context-Awareness to Enhance Source-Location Privacy in Wireless Sensor Networks," *The Computer Journal*, vol. 54, no. 10, pp. 1603–1615, 2011.

[19] Y. Jian, S. Chen, Z. Zhang, and L. Zhang, "A novel scheme for protecting receiver's location privacy in wireless sensor networks," *Wireless Communications, IEEE Transactions on*, vol. 7, no. 10, pp. 3769–3779, October 2008.

[20] M. Shao, W. Hu, S. Zhu, G. Cao, S. Krishnamurthy, and T. La Porta, "Cross-layer Enhanced Source Location Privacy in Sensor Networks," in *IEEE Conference on Sensor, Mesh, and Ad Hoc Communications and Networks (SECON '09)*. IEEE Communications Society, June 2009, pp. 1–9.

[21] B. Alomair, A. Clark, J. Cuellar, and R. Poovendran, "Towards a Statistical Framework for Source Anonymity in Sensor Networks," *IEEE Transactions on Mobile Computing*, vol. 12, no. 2, pp. 248 – 260, 2012.

[22] B. Ying, J. R. Gallardo, D. Makrakis, and H. T. Mouftah, "Concealing of the Sink Location in WSNs by Artificially Homogenizing Traffic Intensity," in *The First International Workshop on Security in Computers, Networking and Communications (INFOCOM Workshops)*, April 2011, pp. 988 – 993.

[23] M. Shao, S. Zhu, W. Zhang, G. Cao, and Y. Yang, "pDCS: Security and Privacy Support for Data-Centric Sensor Networks," *Mobile Computing, IEEE Transactions on*, vol. 8, no. 8, pp. 1023–1038, Aug. 2009.

[24] R. Rios, J. Cuellar, and J. Lopez, "Probabilistic receiver-location privacy protection in wireless sensor networks," *Information Sciences*, vol. 321, pp. 205 – 223, 2015.

[25] Emotiv, Inc. (2014) Wearables for your brain. [Online]. Available: https://emotiv.com/