Seguridad en smart cities e infraestructuras críticas

Victor Garcia-Font
Internet Interdisciplinary Institute
Universitat Oberta de Catalunya
Email: vgarciafo@uoc.edu

Carles Garrigues
Estudis d'Informàtica Multimèdia i Telecomunicació
Universitat Oberta de Catalunya
Email: cgarrigueso@uoc.edu

Helena Rifà-Pous
Estudis d'Informàtica Multimèdia i Telecomunicació
Universitat Oberta de Catalunya
Email: hrifa@uoc.edu

***Resumen*—Numerosas ciudades están desarrollando plataformas smart city con el fin de lograr una mejor coordinación, eficacia, reducción de costes y en general una gestión más eficiente de la ciudad, a través de la integración de infraestructuras y servicios. Entre los subsistemas que se integran en una smart city hay un grupo de especial interés formado por las infraestructuras críticas. Con la integración de estas se busca dar un mejor servicio, pero al aumentar la complejidad y la dependencia de unas infraestructuras con otras y con las TIC, crece el riesgo de que una vulnerabilidad o fallo en una infraestructura pueda extenderse y ocasionar fallos en otra, y así sucesivamente provocando un fallo en cascada.**

En este artículo describimos un diagrama común de muchos proyectos para smart cities y analizamos los problemas de seguridad y privacidad que aparecen al interconectar las infraestructuras y al tender hacia una filosofía de datos abiertos.

***Palabras clave*—ciberseguridad *(cybersecurity)*, ciudad inteligente *(smart city)*, datos abiertos *(open data)*, infraestructura crítica *(critical infrastructure)*, privacidad *(privacy)*, Tecnologías de la Información y la Comunicación *(Information and Communication Technologies)*.**

I. Introducción

En los últimos años, las ciudades han añadido a los retos clásicos nuevos desafíos propios de la sociedad contemporánea: absorción del aumento de la población, reducción del consumo energético y de emisiones de CO2, mayor sostenibilidad, crecimiento económico, etc. Para hacer frente a estos puntos se está produciendo un progresivo aumento de la inversión en capital humano y tecnológico. Usando las TIC como base, llamamos smart city a las ciudades que buscan atajar estos desafíos desarrollando sistemas para la mejora en áreas como la gobernanza, la energía, el medio ambiente, la movilidad o la economía entre otros. El desarrollo de estos sistemas conlleva inherentemente nuevos modelos de operación y modifica características básicas de las ciudades. La implantación de líneas de telecomunicaciones interconecta más a los ciudadanos con las instituciones, a las empresas con sus proveedores, a los gestores de infraestructuras con las infraestructuras que gestionan, etc. Además, esta interconexión también se produce con elementos insertados en el entorno urbano, como por ejemplo cámaras de video vigilancia, sensores, teléfonos móviles, o dispositivos GPS, que generan una gran cantidad de información que pasa a estar disponible no sólo localmente sino a una escala mayor para el conjunto de los entes que conforman la ciudad. Todo esto provoca que se demanden nuevos servicios, se abran nuevas líneas de negocio, se creen nuevos empleos, se puedan automatizar operativas urbanas y mejorar la eficiencia en la gestión de infraestructuras, se haga la ciudad más competitiva y se potencie más transparencia en la gestión pública.

Todos estos cambios que aporta la smart city también afectan a las que llamamos infraestructuras críticas. Éstas son las instalaciones clave que proporcionan los servicios que afectan al bienestar de las personas, sea suministrando directamente estos servicios esenciales, o dando servicio a otra infraestructura crítica para que ésta pueda operar correctamente. Más concretamente, las infraestructuras críticas más destacadas están relacionadas con la energía eléctrica, la producción y distribución de combustibles, las telecomunicaciones, el transporte, la distribución de agua, la agricultura, la banca y las finanzas, los servicios de emergencia y gobernanza, la educación y la sanidad entre otros [1].

Más integración e interconexión trae consigo una mayor complejidad y un mayor riesgo de vulnerabilidades. En este artículo vemos como la implantación de las smart cities abre brechas en la seguridad de la información y en la privacidad de los usuarios. Para empezar, hacemos una descripción a alto nivel de los sistemas de información que se están diseñando para implementar una arquitectura smart city. Posteriormente, vemos como las infraestructuras críticas usan las TIC para interconectarse, integrarse en la smart city y como estas infraestructuras dependen unas de las otras para poder operar. A continuación, revisamos cómo la seguridad informática y la privacidad pueden afectar a la construcción de una smart city. Finalmente señalamos algunos de los problemas que continúan abiertos en estos ámbitos.

II. Smart cities y infraestructuras críticas

II-A. Sistemas de información de una smart city

Los SI de una smart city son el conjunto de software, hardware y estándares que hacen posible la gestión eficiente e inteligente de la ciudad a través de las TIC. En la actualidad, hay diversas compañías y ciudades que han propuesto esquemas de arquitectura smart city. A continuación, mencionamos algunos de los productos que se están construyendo:

The PlanIT Urban Operating System[2] es una implementación de un sistema operativo para entornos urbanos que provee de tecnología en tiempo real de sensores, control, análisis espacial, integración de datos, seguridad, soporte y provisionamiento de contexto de ubicuidad para aplicaciones

ISBN: 978-84-9717-323-0

del internet de las cosas (IoT). Se caracteriza por tener 4 capas: una red de sensores, una capa de control de latencia mínima para el control de los sensores, una capa de supervisión a un nivel más alto y una capa de aplicaciones. Este esquema sigue el paradigma SOA facilitando la creación de aplicaciones que usen sus servicios y la integración de módulos de otros fabricantes.

La ciudad de Oulu en Finlandia [3] ha implementado un middleware para ser usado como campo de pruebas real para mejorar y facilitar la comunicación entre los ciudadanos y el gobierno. Este middleware es una capa encima de la red LAN/bluetooth/wireless de la ciudad para facilitar el acceso a esta red y a los datos generados por sensores distribuidos por el área urbana.

En Corea del Sur están implementando el proyecto *Ubiquitous city* (u-city)[4] en el que ofrecen servicios interconectados distribuidos por áreas de interés: automatización de edificios (u-life), servicios relacionados con los negocios (u-business), gobernanza (u-government), etc. Uno de los puntos principales del proyecto es centrarse en el usuario, ofreciéndole los servicios en cualquier parte pero sin resultar intrusivo.

Chen[5] propone una arquitectura en 4 capas para la integración de la Internet of Things (IoT) en las smart cities. La capa más baja es una red de sensores autónomos que responden a estímulos del mundo real y que interactúan entre ellos. La siguiente capa es un middleware orientado a servicio que sirve como punto de unión entre los sensores y el sistema. La siguiente capa intermedia es una capa de procesamiento de datos. Hay que destacar que se proponen instrumentos para que los diferentes elementos colaboren entre sí para un procesamiento más eficaz. Por ejemplo, un smartphone de poca potencia enviaría parte de un proceso a computar al cloud. Finalmente, se propone una capa de aplicaciones y servicios.

La ciudad de Barcelona está desarrollando un esquema con la integración de varios proyectos [6], [7], [8], [9] cofinanciados por la ciudad y por otras instituciones como la Unión Europea. La capa central de middleware la constituye el *CityOS*, una agregación de módulos para procesamiento, análisis, gestión de datos históricos, BI, etc.

Entre estos módulos dentro del *CityOS* de Barcelona se encuentra el *City Service Development Kit* (*CitySDK*)[6]. Este proyecto tiene el objetivo de ayudar a las ciudades a abrir sus datos dando un conjunto de herramientas open source para facilitar a los desarrolladores la creación de servicios digitales para la ciudad. Estas herramientas son básicamente servicios digitales abiertos e interoperables, procesos, guías y estándares de usabilidad. *CitySDK* no es solamente un módulo integrado en la smart city de Barcelona, sinó que también se ha integrado en la arquitectura de otras ciudades y busca ser una pieza para que cualquier ciudad europea pueda ofrecer sus datos a desarrolladores para la creación de aplicaciones y así contribuir a la creación de una infraestructura sostenible de apps. Como colofón del proyecto, se desarrollan tres aplicaciones en los ámbitos de la participación ciudadana, el turismo y la movilidad integrados en las smart cities de Helsinki, Lisboa y Amsterdam.

En general, todas las propuestas existentes en smart cities tienen una arquitectura orientada a servicio (SOA) con una pieza central que actúa de middleware y que en muchas de las propuestas se equipara a un sistema operativo con un ámbito de ciudad. En la figura 1 se puede ver un diagrama general de bloques para una solución de este tipo. Básicamente se trata de arquitecturas en tres capas: capa de aplicaciones, capa de proceso y capa de contacto con el medio.

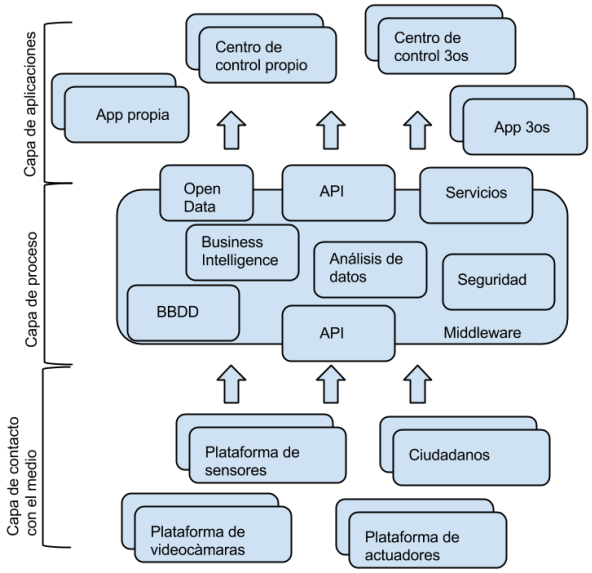

Figura 1. Diagrama de bloque general de una smart city

En la capa de aplicaciones situamos todos los elementos que usan los servicios y la información publicada por la smart city. Por ejemplo, centros de control o aplicaciones.

La capa central se trata de un middleware compuesto por muchos módulos de diversos tipos, diferentes funcionalidades e implementados por entidades diferentes que se comunican entre ellos con el uso de estándares, como por ejemplo el API REST. Las soluciones de smart city, tanto las basadas en open source como las propietarias hacen hincapié en el uso de estándares y la interoperabilidad ya que la finalidad de los sistemas de este tipo es la concentración de subsistemas y la generación de nuevos datos para ser usados en aplicaciones de diversa índole. Generalmente, el middleware aparte de ser el nexo de unión entre sensores, actuadores y aplicaciones, también es una pieza para el procesamiento, el almacenaje, la gestión y el análisis de datos. Gracias a la interoperabilidad de estos sistemas se busca poder encajar cualquier tipo de producto que dé estos servicios, como sistemas de ERP, de Business Intelligence, sistemas gestores de bases de datos o minerías de Big Data.

La capa de contacto con el medio corresponde a los elementos que alimentan con información al sistema o que el sistema usa para interactuar con los componentes de la ciudad, como por ejemplo los sensores, los actuadores o los propios ciudadanos. Dentro de esta capa, destacamos los módulos de

plataforma de sensores. En este sentido, el proyecto de open source *Sentilo*[8], implementado y desplegado en la ciudad de Barcelona, ofrece una API REST en la que se suscriben los sensores y los actuadores. Así, los sensores envían la información recogida a la plataforma de sensores para que sea procesada por agentes del sistema y reenviada hacia una capa superior o para que sirva de información de reentrada. Las funciones de suscripción y notificación crean un medio para la conexión de sensores y actuadores escalable.

II-B. Las infraestructuras críticas de una smart city

De entre todas las infraestructuras críticas, en este artículo nos centramos en las que tienen un impacto mayor en las ciudades, y por lo tanto, las que entran en el ámbito y son candidatas a ser integradas en un esquema de smart city. Más concretamente, dentro de una ciudad las infraestructuras críticas más relevantes son las energéticas, las de telecomunicaciones, la distribución de agua, la gobernanza, los servicios de emergencia y seguridad pública, el transporte y la sanidad[10].

Estas infraestructuras críticas han ido evolucionando su manera de operar y sus centros de control, empezando con una gran dependencia de acciones manuales y tendiendo a la automatización. Para ello, se han adaptado o reemplazado los antiguos mecanismos de control por nuevos dispositivos informatizados dándoles conectividad IP y uniéndolos a redes de ordenadores para poder ser operados a distancia. Esta informatización también ha llevado a una interconexión entre las diversas infraestructuras que no existía previamente, pudiéndose enviar y recibir información de unas a las otras para ganar en coordinación y cooperación.

A parte de la interconectividad que se produce al informatizar las infraestructuras, también tenemos que considerar las dependencias naturales - o interdependencias en el caso de que haya dependencias recíprocas - que existen entre ellas. Éstas pueden deberse a una causa de tipo física, TIC, geográfica o lógica[1].

Una dependencia física es aquella que conecta dos infraestructuras porqué una necesita lo que suministra la otra para poder operar. Por ejemplo, necesitamos que la producción de energía eléctrica funcione correctamente para poder mantener activo el servicio de telecomunicaciones.

Una dependencia TIC se da en las infraestructuras que necesitan de la información transmitida por otra infraestructura a través de la infraestructura de telecomunicaciones. Este tipo de dependencia va en aumento debido a la extensa utilización de los sistemas de control industrial para la Supervisión, Control y Adquisición de Datos (SCADA). Además, los centros de control que gestionan las infraestructuras tienden a estar cada vez más alejados de las infraestructuras que controlan, con lo que la dependencia con las TIC es todavía más enfatizada.

Las dependencias geográficas se encuentran en esos puntos en que se sitúan próximamente varias infraestructuras críticas, por ejemplo un puente donde pasan líneas de comunicaciones o canalizaciones de agua. Una afectación en el puente podría provocar problemas tanto en las líneas de tráfico, como en las telecomunicaciones o el suministro de agua.

Finalmente, las dependencias lógicas son aquellas que existen entre dos infraestructuras y que no corresponden ni a dependencias de tipo físico, ni TIC, ni geográfico. En este caso un agente en una infraestructura depende de algún modo de un agente en otra, pero el vínculo entre los dos se establece por algún mecanismo que no corresponde a los anteriormente mencionados. Un ejemplo de este tipo es la dependencia que se produce entre las infraestructuras eléctricas y las financieras. Desde la privatización del mercado eléctrico se han hecho muchas inversiones financieras en este sector. Por consiguiente, se producen cuantiosas pérdidas financieras cuando hay afectaciones en el precio de la energía, del transporte, al aplicar nueva regulación, nuevos impuestos, etc. Igualmente, afectaciones en los mercados financieros que hagan desplazar las inversiones en el sector eléctrico pueden no hacer rentables algunas plantas generadoras y desproveer a la red eléctrica de potencial.

En relación a los tipos de dependencia, cabe mencionar la clasificación respecto al nivel de criticidad que tiene un fallo y la temporalidad que ese fallo conlleva. La interrupción de producción de energía eléctrica en una planta de mediano tamaño puede no afectar demasiado al sistema en un día de poco consumo, pero ese mismo fallo puede llevar a una caída en cadena del sistema en un día con un pico de consumo. Además, también hay que distinguir en el grado de acoplamiento que tienen las infraestructuras. Por ejemplo, el corte de suministro de gas a un generador de ciclo combinado probablemente tendrá consecuencias casi inmediatas en la generación de energía eléctrica. En cambio, en las centrales de carbón, al disponer normalmente de reservas, un corte en el suministro no tendrá una consecuencia hasta al cabo de varios meses.

La conjunción de las tres características anteriores: incorporación de sistemas TIC, dependencias y mayor interconexión entre infraestructuras es la base de funcionamiento de un sistema smart city. Una vez establecida la interconexión, el sistema smart city se encarga de analizar las dependencias entre las infraestructuras con los datos en tiempo real provenientes de sensores y otros dispositivos repartidos por la ciudad y así ofrecer herramientas para un mejor control y operación de los diferentes servicios. Por ejemplo, una red de sensores en las calles que monitoreen el tráfico podría enviar información detallada del número de vehículos circulando por determinadas vías al centro de control de tráfico. Varias operaciones de análisis y predicción podrían alertar de los atascos y de las vías más rápidas. Esta información sería enviada al centro de control de ambulancias que combinando estos datos con los sistemas de posicionamiento planificaría las unidades mejor situadas para atender una urgencia y las rutas a tomar. En un sistema altamente conectado el centro de control de emergencias también podría enviar información al de tráfico sobre las intervenciones necesarias, que introducido en la red semafórica podría seguir el recorrido de los servicios de emergencia y darles prioridad.

II-C. Los datos y la información en una smart city

Una de las particularidades más destacadas de las smart cities es la gran cantidad de datos que manejan provenientes de fuentes heterogéneas distribuidas geográficamente por el área urbana. Si listamos estas fuentes clasificándolas con el vínculo que tienen con la identidad y la privacidad de los ciudadanos tenemos:

- **Fuentes no personales** correspondientes a los dispositivos que registran datos que no tienen ningún vínculo estrecho con una persona en concreto. E.g., sensores de temperatura, de humedad, sonómetros.
- **Fuentes personales** son aquellas vinculadas a un usuario donde su identidad aparece directamente. El ciudadano puede haber dado la información activamente, e.g., la participación en una aplicación de denuncia ciudadana, o de forma inconsciente sin saber que su información acabaría dentro del sistema, e.g., un comentario en una red social que es analizado por el sistema.
- **Fuentes anónimas** ofrecen datos que provienen de los usuarios pero se han tratado previamente para enmascarar la información personal de éstos. E.g., cámaras de videovigilancia que ensombrecen rostros, un parquímetro realizando la lectura de la matrícula de un coche. Hay que tener en cuenta que dependiendo de cómo se haya hecho el tratamiento de datos se podría deducir información de algunos usuarios. E.g., datos de consumo eléctrico en agregaciones espaciales de unos pocos kilómetros cuadrados pueden no revelar información sobre habitantes de regiones densamente pobladas, pero puede no ser suficiente para áreas rurales.

Cada vez hay más dispositivos que pueden nutrir datos al sistema smart city y a esto hay que añadir el movimiento open data. Este movimiento promueve que cada vez haya más datos que se abran. En muchos casos, para respetar la privacidad del ciudadano, la información se presenta agregada o anonimizada. Así, este modelo de más datos y más abiertos ayuda a la transparencia de las administraciones y empresas de servicio público, es fuente de creación de nuevas aplicaciones y servicios, pero también añade incertidumbre sobre los datos que se ofrecen y la manera en que se ha hecho el tratamiento de datos privados.

III. Seguridad y privacidad

Sin tener en cuenta los problemas derivados de las numerosas interconexiones y dependencias inherentes a una smart city, este tipo de sistemas también afrontan los problemas de seguridad informática clásicos que afectan a los centros de datos y a los sistemas de comunicación: malware (virus, troyanos, gusanos, backdoors, spyware), bots, loggers, rootkits, ataques de denegación de servicio distribuidos (DDoS), falta de actualizaciones, etc. Se han destacado los gusanos y los DDoS como los más peligrosos para los servicios que ofrece la smart city en tiempo real y para las infraestructuras críticas, ya que tienen una afectación muy alta para el rendimiento de los sistemas[11]. Típicamente, la prevención contra todos estos ataques se ha hecho con la instalación de antivirus, firewalls, honeypots, sistemas de detección de intrusiones (IDS), la creación de políticas de seguridad, la actualización de los sistemas y la implementación de medidas de autenticación. Los problemas de falta de actualización son de especial relevancia en las infraestructuras críticas, donde precisamente por su criticidad se minimizan las actualizaciones para evitar daños[12]. También hay dificultades para la actualización, la aplicación de nuevas políticas de autenticación o la denegación de autorizaciones en los dispositivos repartidos por la ciudad y que no disponen de una plataforma común de control.

En el ámbito de la privacidad, los problemas tradicionales que conciernen a las smart cities afectan a las bases de datos, a la identidad de los usuarios y a las comunicaciones.

En el campo de las bases de datos hay algunos procedimientos propuestos dirigidos a mantener la privacidad de los usuarios[13]. Las técnicas de Statistical Disclosure Control (SDC) proponen añadir ruido o hacer agregaciones para preservar la privacidad pero a su vez manteniendo el valor informativo de los datos. Las técnicas de Private Information Retrieval (PIR) se basan en hacer consultas pidiendo más información de la necesaria para ocultar la información concreta que demandaba el usuario. Otras técnicas como el cloaking y el uso de pseudónimos se usan para ocultar la identidad de los usuarios concretos al acceder a servicios basados en la localización (LBS).

Para los problemas de privacidad en las comunicaciones, la criptografía avanzada y el control de acceso son los sistemas usados para la prevención de escuchas en la transmisión de datos y para evitar la conexión de nodos no autorizados en las redes con aparatos distribuidos en lugares de acceso público[14]. Sin embargo, el uso de técnicas criptográficas puede ser viable para dispositivos con alta capacidad de cómputo, como los contadores inteligentes, pero sensores y otros dispositivos más pequeños pueden no tener capacidad suficiente para realizar estas funciones.

III-A. Problemas abiertos

La complejidad de un sistema crece exponencialmente al añadir nuevos subsistemas, y el número de vulnerabilidades que añade al conjunto este nuevo subsistema es mayor que las que lo afectaban de forma aislada[14]. Estas vulnerabilidades pueden ser aprovechadas por hackers o terroristas no sólo para causar daño al sistema que tiene abierta esta vulnerabilidad, sino que pueden utilizarla como puerta de entrada al resto de subsistemas que conforman la smart city.

El primer problema aparece al aumentar las interconexiones entre servicios, empresas e infraestructuras, ya que incrementamos también las vías para la circulación de virus entre objetivos codiciados como son las infraestructuras críticas. El ejemplo de infección del gusano Stuxnet[15] que ha afectado a los sistemas de control industrial aprovechándose de vulnerabilidades en sistemas Windows nos muestra la fragilidad y el riesgo de implantar las TIC e interconectar este tipo de entornos que anteriormente tenían su seguridad basada básicamente en seguridad física para impedir el acceso. Cómo los

virus, los hackers también pueden utilizar las interconexiones para viajar entre sistemas y ganar control.

El segundo problema en un sistema smart city procede de las dependencias entre infraestructuras. Un fallo en uno de los nodos en la red de dependencias podría causar problemas en cascada a varias infraestructuras críticas. Para una mejor planificación y gestión de las dependencias se han propuesto soluciones en el campo de la simulación y el modelado, pero los productos que sirven para una gestión global de múltiples infraestructuras están todavía poco maduros[16]. Este tipo de problemas en cascada puede deberse tanto a la disrupción de uno de los subsistemas como a la generación de desinformación. Continuando con el ejemplo de la sección II-B, si un atacante produjera un colapso en uno de los colectores que recoge los datos de los sensores de tráfico de un cruce importante y a su vez provocara una pequeña incidencia circulatoria, no solamente estaría afectando a las lecturas de tráfico, sino que el servicio de ambulancias estaría basando su planificación en datos desactualizados.

En tercer lugar, la conexión entre el middleware de la smart city y el resto de plataformas y aplicaciones es un elemento estratégico para que una smart city tenga éxito. Esta conexión tiene que ser interoperable, estandarizada y a su vez contemplar los principios básicos de confidencialidad, integridad y autenticidad. Por lo tanto, las APIs que ofrece la plataforma tienen que soportar el uso de protocolos con encriptación como HTTPS, hecho que crea algunos problemas. Por ejemplo, la posibilidad de que un atacante use un dispositivo en la vía pública con una conexión encriptada para enviar un virus hasta el subsistema de la smart city que desencripta la conexión. En este caso, un firewall perimetral no podría descifrar el contenido enviado y por lo tanto no podría detectar el virus. Un segundo ejemplo recae en que algunos dispositivos por su poca capacidad no soportan conexiones encriptadas. Aceptar que también sean posibles este tipo de conexiones para dispositivos inocuos abre la puerta a que sean atacados y también a errores humanos como malas configuraciones en otros elementos más peligrosos.

Un cuarto problema aparece con el hecho de disponer de muchos servicios y fuentes de datos para la creación de nuevas aplicaciones. Esto es una ventaja, pero a su vez es un riesgo al no poder asegurar la disponibilidad de estos servicios. Por ejemplo, una aplicación para la visualización del servicio de autobuses donde aparezcan las líneas y las paradas de autobús en un mapa cerca de la zona donde estamos con el tiempo de espera para cada autobús podría necesitar la disponibilidad de un servidor de mapas, de un servicio de localización para indicar al usuario donde se encuentra y del servicio que da información de forma dinámica en tiempo real sobre el tiempo de espera de los autobuses. Un fallo en cualquiera de estos servicios llevaría a la aplicación a no funcionar debidamente o incluso a que fuera inservible.

Finalmente, en el ámbito de la privacidad, a pesar de las técnicas mencionadas en la sección III, en un contexto de open data con cuantiosas fuentes de información tanto en tiempo real como históricas, al publicar nuevos datos parece difícil poder asegurar que no podrán ser utilizados para inferir la identidad de los usuarios al aplicar alguna técnica de correlación en el futuro. Un ejemplo del uso de técnicas de este tipo lo ha llevado a cabo la ciudad de Nueva York[17]. Para no tener que pagar para deshacerse de los aceites usados, algunos restaurantes los vierten ilegalmente en las alcantarillas. Correlacionando datos públicos provenientes del sistema de alcantarillado, información de contaminación, de licencias de restaurantes, de compañías de recogida de residuos entre otras, el ayuntamiento pudo dibujar un mapa de probabilidades de los restaurantes que habían cometido los vertidos ilegales sin disponer de ningún dato inicial que indicara la identidad de los autores.

Para disminuir el tiempo en las intrusiones y en los ataques, se propone la implantación de soluciones capaces de aplicar reacciones activas donde automáticamente el sistema responda en un escenario de crisis para frenar una anomalía[18]. Estas soluciones son todavía poco comunes, ya que los sistemas actuales están basados en la activación de alertas para la solución semimanual de irregularidades.

IV. Conclusión

En este artículo hemos presentado un esquema genérico de smart city en el que se basan algunos de los productos implementados por empresas y ciudades. A partir de este esquema, hemos repasado cómo se están integrando las infraestructuras críticas a la smart city a base de informatizarlas e interconectarlas. A las dependencias naturales que tienen entre sí estas infraestructuras, se le añaden dependencias con las TIC, que llevan a todo el sistema a ser más vulnerable a ciberataques y a ser susceptible a fallos múltiples en cascada. Así, hemos repasado los problemas de seguridad informática que el modelo de smart city tiene asociado. Además, el paradigma de open data en el que se basa la publicación de muchos de los datos generados por la smart city contrae problemas de privacidad para los ciudadanos y las empresas de las que se extraen esos datos. Varios de estos problemas de seguridad y privacidad han sido resueltos para otros entornos, pero debido a las particularidades y características propias de una smart city, algunos de los problemas continúan abiertos en este contexto.

Agradecimientos

Este trabajo está financiado parcialmente por el Ministerio de Economía y Competitividad a través de los proyectos TIN2011-27076-C03-02 “CO-PRIVACY” y CONSOLIDER INGENIO 2010 CSD2007-0004 “ARES”; y por la Generalitat de Catalunya a través de la subvención de doctorado industrial ECO/2497/2013. Merecen un agradecimiento especial el Ayuntamiento de Barcelona, Cast Info y openTrends.

Referencias

[1] S. M. Rinaldi, J. P. Peerenboom, and T. K. Kelly, “Identifying, understanding, and analyzing critical infrastructure interdependencies,” *Control Systems, IEEE*, vol. 21, no. 6, pp. 11–25, 2001.

[2] “Living planit os,” http://living-planit.com/UOS_overview.htm, accessed: 2014-03-27.

[3] F. Gil-Castineira, E. Costa-Montenegro, F. J. Gonzalez-Castano, C. López-Bravo, T. Ojala, and R. Bose, "Experiences inside the ubiquitous oulu smart city," *Computer*, vol. 44, no. 6, pp. 48–55, 2011.
[4] Y. W. Lee and S. Rho, "U-city portal for smart ubiquitous middleware," in *Advanced Communication Technology (ICACT), 2010 The 12th International Conference on*, vol. 1. IEEE, 2010, pp. 609–613.
[5] M. Chen, "Towards smart city: M2m communications with software agent intelligence," *Multimedia Tools and Applications*, vol. 67, no. 1, pp. 167–178, 2013.
[6] "Citysdk," http://www.citysdk.eu/, accessed: 2014-03-27.
[7] "icity," http://www.icityproject.com/, accessed: 2014-03-27.
[8] "Sentilo," http://www.sentilo.io/wordpress/, accessed: 2014-03-27.
[9] "Open cities," http://opencities.net/, accessed: 2014-03-27.
[10] F. Ferraz, C. Sampaio, C. Ferraz, G. Alexandre, and A. Carvalho, "Towards a smart city security model exploring smart cities elements based on nowadays solutions," in *ICSEA 2013, The Eighth International Conference on Software Engineering Advances*, 2013, pp. 546–550.
[11] C.-W. Ten, G. Manimaran, and C.-C. Liu, "Cybersecurity for critical infrastructures: attack and defense modeling," *Systems, Man and Cybernetics, Part A: Systems and Humans, IEEE Transactions on*, vol. 40, no. 4, pp. 853–865, 2010.
[12] F. Daryabar, A. Dehghantanha, N. I. Udzir, N. F. B. M. Sani, and S. bin Shamsuddin, "Towards secure model for scada systems," in *Cyber Security, Cyber Warfare and Digital Forensic (CyberSec), 2012 International Conference on*. IEEE, 2012, pp. 60–64.
[13] A. Martinez-Balleste, P. A. Pérez-Martínez, and A. Solanas, "The pursuit of citizens' privacy: a privacy-aware smart city is possible," *Communications Magazine, IEEE*, vol. 51, no. 6, 2013.
[14] A. Bartoli, J. Hernández-Serrano, M. Soriano, M. Dohler, A. Kountouris, and D. Barthel, "Security and privacy in your smart city," in *Proceedings of the Barcelona Smart Cities Congress*, 2011.
[15] R. Langner, "Stuxnet: Dissecting a cyberwarfare weapon," *Security & Privacy, IEEE*, vol. 9, no. 3, pp. 49–51, 2011.
[16] S. M. Rinaldi, "Modeling and simulating critical infrastructures and their interdependencies," in *System sciences, 2004. Proceedings of the 37th annual Hawaii international conference on*. IEEE, 2004, pp. 8–pp.
[17] T. G., "Why grease is the word in new york," http://www.ft.com/cms/s/2/a284331a-9751-11e2-a77c-00144feabdc0.html#axzz2P5yLBdjC, 2013, accessed: 2014-03-27.
[18] L. Cazorla, C. Alcaraz, and J. Lopez, "Towards automatic critical infrastructure protection through machine learning," in *Critical Information Infrastructures Security*. Springer, 2013, pp. 197–203.