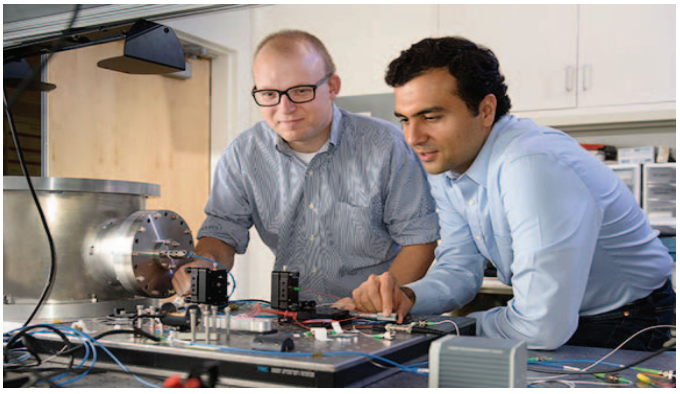
Nueva computadora combina circuitos electrónicos con pulsos de luz

(Fuente: New Computer Combines Electronic Circuits with Light Pulses, By Jeremy Hsu, Oct 2016, IEEE Spectrum Tech Talk)



El problema clásico del "vendedor viajero" es un problema de optimización que resulta fundamental en investigación de operaciones y ciencia computacional teórica, así como para muchas aplicaciones del mundo de los negocios, tales como la planificación de las rutas de camiones de reparto o el descubrimiento de nuevas drogas farmacéuticas. Actualmente, se tiene la limitación de que los computadores modernos todavía no tienen la capacidad para encontrar la mejor solución a este tipo de problema; y es que, aun encontrar soluciones aproximadas, es exigente.

En la actualidad, los computadores manejan los problemas de optimización combinacional saltándose algunas de las soluciones más débiles en lugar de considerar todas las posibilidades para encontrar la mejor solución. Por esto, un grupo de científicos de E.U. y Japón han desarrollado un nuevo computador especializado que podría algún día solucionar el problema del "vendedor viajero" y problemas similares en forma más eficiente. Es una máquina híbrida que combina circuitos electrónicos digitales con dispositivos ópticos similares al láser.

Con el nuevo computador se busca solucionar problemas de optimización usando un modelo matemático conocido como "modelo Ising", el cual describe como los materiales magnéticos tienen espines atómicos que existen en estados ya sea arriba o abajo. Al imitar un arreglo de tales magnetos minúsculos, el computador especializado "máquina Ising" puede representar un problema de optimización como una configuración única de estados arriba o abajo de espín, en los que cada uno interacciona con otro por medio de acoplamientos. Es por medio de los acoplamientos entre espines, que se codifica el problema que se quiere resolver, y la solución de la "máquina Ising" es idealmente la configuración del estado fundamental que minimiza la energía total del sistema, dado el conjunto de acoplamientos.

Por muchos años, ingenieros y físicos han experimentado con diferentes computadores tipo "máquinas Ising" para resolver tales problemas de optimización, usando diferentes estrategias, entre las que se tiene: redes neuronales inspiradas en el cerebro construidas con circuitos electrónicos; computación cuántica adiabática que involucra máquinas de "recocido" cuántico de ondas-D, y problemas de optimización de codificación dentro de moléculas de ADN biológico como una forma de computación molecular.

Pero el equipo de científicos de EE.UU. y Japón han tomado una estrategia bastante diferente para construir las "máquinas Ising". Ellos utilizan pulsos de luz de un dispositivo similar a un láser, llamado oscilador paramétrico óptico, para representar los espines magnéticos. Estos pulsos de luz son medidos individualmente y combinados unos con otros para formar sistemas más grandes que simulan arreglos de magnetos minúsculos. Para controlar y combinar los pulsos de luz, se requieren líneas de retraso ópticas y moduladores ópticos. Pronto, se dieron cuenta que una máquina completamente óptica resultaba muy costosa y difícil de escalar, debido a las líneas de retraso y los moduladores, por lo que optaron por una máquina híbrida, parte electrónica digital y parte óptica, donde la interacción que ocurre entre los pulsos de luz se simula con circuitos electrónicos, y luego la información se traduce y se pasa a la porción óptica del sistema.

Se han hecho pruebas exhaustivas con múltiples versiones de problemas de optimización para demostrar que las soluciones no están limitadas a problemas específicos, y se han usado diferentes números de espines para evaluar las capacidades y el desempeño.

La gran pregunta con esta versión de la "máquina Ising" es si ésta puede vencer a los mejores algoritmos que corren en computadores clásicos. Los resultados publicados hasta la fecha son prometedores, pero en los próximos años, los grupos de investigación estarán realizando pruebas de comparación de velocidad, y también para clarificar las ventajas y desventajas de la "máquina Ising" sobre los computadores convencionales. Además, se estará abordando la aplicación de estas máquinas a aplicaciones comerciales del mundo real, como la optimización de redes de comunicación móviles o el descubrimiento de nuevas configuraciones de moléculas para nuevas drogas farmacéuticas.

Nuevo reloj inteligente que se carga con el calor de la piel

(Fuente: This Smart Watch Will Charge Itself Using Heat From Your Skin, by Tekla S. Perry, Nov 2016, IEEE Spectrum Tech Talk)

¿Cuántos olvidamos cargar las baterías de nuestros monitores de actividad física, perdiendo luego la información y la motivación? Matrix Industries, con base en California, ha indicado que tiene la forma de solucionar esto. Y es que piensan que la tecnología termoeléctrica está lista para alimentar los dispositivos portátiles, y pronto permitirá proveer

energía para dispositivos implantables y sensores de baja potencia para el Internet de las Cosas. Los dispositivos termoeléctricos recolectan energía usando la diferencia de temperatura entre sus dos lados para generar un voltaje.

Matrix ha lanzado lo que llama un reloj inteligente con alimentación termoeléctrica. Este dispositivo tiene un contador de pasos, un contador de calorías gastadas, un monitor de sueño, y por supuesto, un reloj para el tiempo. Aunque estos dispositivos son atractivos para los consumidores jóvenes y aquellos que les gusta lucir lo último, no son el objetivo principal de Matrix. La empresa está realmente interesada en convencer a otros fabricantes de artefactos que adopten su tecnología termoeléctrica.

"Nosotros nos vemos como una compañía de recolección de energía térmica", indica Anne Ruminski, jefe de ingeniería de Matrix, "no como un fabricante de relojes". Lo que se quiere es que la tecnología termoeléctrica de Matrix se adopte para otros dispositivos portátiles, dispositivos médicos y sensores inteligentes.

Ruminski indica que es el momento oportuno para usar la energía termoeléctrica en dispositivos portátiles, y que están sorprendidos de que, cuando buscan en las aplicaciones para esta tecnología, todos están trabajando enfocados en usarla en autos, lo que aún no es factible. Están sorprendidos de que nadie la ha puesto en un reloj. "Los relojes inteligentes tienen sentido, porque los dispositivos que van en los relojes inteligentes de hoy utilizan mucho menos energía que hasta hace solo un par de años atrás".

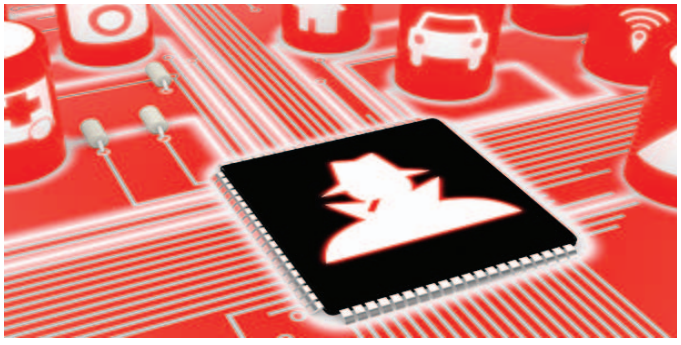
La compañía apunta a la implementación de la tecnología en dispositivos de ayuda auditiva, e indican que es especialmente adecuada para dispositivos implantables, como los marcapasos.

Matrix ha llenado patentes en aplicaciones termoeléctricas y en administración del calor. Ruminski indica que "encontrar la forma de cómo manejar el calor de manera que el lado frío del sistema no se caliente, fue un gran reto".

Se demanda un marco regulatorio para la seguridad del internet de las cosas

(Fuente: Wanted: Smart Public Policy for Internet of Things Security, by Amy Nordrum, Nov 2016, IEEE Spectrum)

Sin que usted lo sepa, los dispositivos conectados en su hogar y negocio pueden estar llevando a cabo acciones maliciosas. Cada vez más, el internet de las cosas (IoT – Internet of Things) se ha convertido en un arma para los hackers. Esto es posible en gran medida por culpa de los fabricantes al no programar medidas de seguridad básicas en estos dispositivos.



Ahora, expertos en EE.UU. están pidiendo a los reguladores que intervengan. La demanda de que la política pública mejore la seguridad de los dispositivos ha alcanzado un punto álgido después de una serie de ataques de denegación de servicio de alto perfil a través de *DVRs, routers y Webcams* no sospechosos. En octubre, los *hackers* inundaron con tráfico el servicio de Internet de una compañía, uniendo millones de dispositivos del IoT en un *botnet virtual* usando un programa malicioso llamado Mirai.

Bruce Schneier, un especialista en seguridad afiliado a la Universidad de Harvard, que pide mayor regulación, indica que "estos problemas no son problemas que los mercados puedan resolver". Dice que los ataques como el indicado arriba son similares a la contaminación del aire – "son una externalidad que los fabricantes no están motivados a solucionar".

En vista de los ataques recientes, queda claro que los dispositivos del IoT continuarán sirviendo como una primera línea para crear *botnets* si su seguridad no se mejora. Se hace necesaria entonces la regulación ya que los fabricantes no están haciendo lo que es importante para el interés común, y se limitan a lo que es importante para su interés comercial.

Sin embargo, la regulación es un caso complicado, ya que el término IoT abarca miles de millones de dispositivos conectados a Internet, que van desde simples sensores a supercomputadores, y la regulación de todos ellos implicaría abarcar múltiples sectores diferentes entrelazados. Hasta el momento, no ha habido una propuesta clara o un acuerdo entre los que apoyan un potencial marco regulatorio para la seguridad del IoT. Además, hay muchos que difieren y piensa que una regulación de gobierno no será efectiva ya que los *hackers* cambian frecuentemente sus ataques y ninguna regulación podría seguir estos cambios.

Al consultar con expertos sobre ciberseguridad, *están indican* que no está claro qué se debe hacer en términos de regulación, pero lo que sí es obvio es que el mercado no puede resolverlo. Un aspecto importante en este tema es si existe una agencia que claramente tenga la autoridad para regular e imponer cualquier nueva reglamentación, si es que esta se establece. Hasta ahora, no hay ninguna agencia encargada de darle seguimiento al IoT, en lugar de esto, algunas agencias han encontrado alguna razón para cubrir parte de ello. Así por ejemplo, el Departamento de Servicios de Salud y Humanos protege la información de salud personal almacenada en dispositivos conectados, mientras que la Reserva Federal ha publicado una guía de seguridad que cubre dispositivos asociados a la industria financiera, entre otros.

Una posibilidad para avanzar en una legislación para mejorar la seguridad del IoT es la de una regulación flexible, la cual describa pasos críticos que las compañías debe seguir, tales como realizar valoraciones de riesgo, preparar planes para minimizar riesgos de seguridad, etc., y que las compañías sean penalizadas si no cumplen con los mismos.

Lo que está claro es que mejorar la seguridad del IoT es un asunto complicado pero crítico.